



# SWEN-331 Insider Threat

Number of Respondents: 68


## 1. Did you enjoy the activity?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Not Applicable
	0	2	10	37	18	1


## 2. How much did you learn in the activity?

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Not Applicable
	0	2	11	39	14	2


## 3. How well do you feel the activity has prepared you for the real world

	Extremely Poor	Below Average	Average	Above Average	Excellent	Not Applicable
	0	3	31	23	10	1

## 4. How likely would you be to recommend the activity to a friend?


	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Not Applicable
	0	6	15	29	16	2

## 5. Do you feel like the activity prepared you for the notion of "Insider Threat"

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Not Applicable
	2	1	4	39	21	1

## 6. Do you feel you are more prepared to deal with "Insider Threat" than before the activity

	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Not Applicable

	0	4	9	38	16	1
--	---	---	---	----	----	---

## 7. Do you feel the activity was done at the appropriate place in the term?

---

- Yes.
- Sure.
- Yes
- Yes
- Yes
- Sure
- Yes
- Yes
- yes
- Yes
- sure
- Yes
- I believe it would be more reasonable to do it near week 7-8.
- Yes, it was unexpected (as it should be) but perfectly introduced us into the notion.
- No, it was due the same day as a major project.
- Yes this time in the semester makes sense for it
- Sure.
- Yes
- Yes
- Yes.
- yes
- Yes
- Yes due to the fact that we have learned at least some of the basic issues that can arise when dealing with software security.
- Yes
- I believe the timing of the activity was appropriate. During week 10, you have a solid foundation of the skills and methodologies to be wary of the "insider threat".
- Yes but it could have been earlier or later. As long as the students learned threat modeling.
- Yes, I think everyone has been extremely busy the past few weeks and therefore were more vulnerable to an insider threat.
- Yes.
- Yes
- Yup, any time is a good time for this one IMO.
- Yes
- Yes.
- Yes
- Yes
- yes

- Yes
- Yes
- Yes
- yes
- Yes
- Yes, we had a decent understanding of security threats at this point in the term.
- Besides for the beginning of the class before we've talked about anything, there really wasn't an inappropriate time for this activity.
- Yes
- Yes
- Yes.
- Yes
- Yes
- Yes.
- Yes, it fit in well.
- Yes
- Sure
- Yes
- Yes
- Yes
- Yes
- Yes
- Yes
- Yes
- Yes.
- Yes
- Yes. It was helpful knowing something about security before embarking on this activity adventure.
- Yes
- Yes
- Yes.

**5 users did not answer**

## **8. What did you like most about the activity?**

---

- Alerted me that malicious insiders are not obviously so.
- I got to be the insider threat.
- It was really interesting to see how few people were looking for an insider threat and many threats went completely unnoticed. It showed that we weren't prepared to consider our classmates as threats.
- How much of a surprise it was, I think that was key to making this activity work.
- It was not expected. This was good. It mixed things up and I think captured people's attention better than just having a standard lecture on the topic.

- The surprise not only teaches the lesson but leaves an impression. This is probably due to the deception aspect of the activity. If you think of the amount of lessons a student receives between kindergarten and graduating college its really not surprising that school can become rather monotonous. This lesson provided a good contrast.
- It was different than other activities previously done in class
- I didn't
- That it made us think about a new kind of threat
- I liked that nobody knew what was going on until it happened.
- The thing with the guy who was bad.
- Finding out that Bryon wasn't just being incompetent, he was being incompetent on purpose.
- The example case studies were hilarious to read.
- It was extremely unexpected, because I never really thought of threats within your team before.
- The incidents we read about were interesting.
- The cases in our part of the study were very interesting. Particularly the porn one
- Being the insider threat without my team knowing.
- No one was aware of it happening
- The reveal of actual insider.
- It was an authentic insider threat
- I liked how the insider threats were unsuspected and in most cases undiscovered.
- The fact that it really did represent an insider threat that I would have otherwise not been exposed to.
- The discussion about how the moles created vulnerabilities
- I enjoyed listening to how other "insiders" confiscated their team's system.
- I liked how it showed me how easily insider threat can destroy a project. During the big reveal I was really nervous that the traitor would be person A who designed most of the threat model. I also can use more threat model experience because I am bad at it so that was nice.
- The reveal that there were insiders
- Researching case studies.
- The subtlety of a mole being placed in each group only to later be exposed. (The reality of the situation)
- Easy, simple, proved a point.
- Great premise - the mole was a huge surprise for our team and a valuable learning experience about insider threats.
- Was interesting to hear what each of the moles tried to do.
- not knowing about the team member being an insider was pretty good, especially with no knowledge that that was what the activity was about
- We didn't even know that there could be a mole, so it was accurate to the real threat.
- It was a fun way to simulate an insider threat.
- The domain we were working in was familiar to us (student grading system).
- The big reveal that there were moles in each group.
- The mole reveal shows how people could have malicious intentions when you least expect it
- The surprise
- I learned better by actually doing it.

- That it was a surprise as to the true intent
- I like how we had to design the system from the ground up and incorporate security into the design
- The examples
- The surprise moles in the groups.
- Didn't even know there were moles
- I was a mole. It was enjoyable to see the other side of the issue.
- Case stories and other forms of insider stories
- The fact that we didn't know ahead of time, that there was a mole in this activity as opposed to knowing there was one but not knowing who.
- Wasn't a fan overall
- Looking at others designs
- I liked that we were shown an obvious problem in the project that we assume won't happen to us.
- It was unexpected.
- I thought it was interesting that not many people realized there was a mole in the group.
- I liked the insider thread twist. It added a cool layer of intrigue to the assignment.
- Really didn't see it coming.
- Mole stories
- I had no idea there was a mole on the team, and the reveal made a very strong point about insider threats.

**12 users did not answer**

## **9. What did you like least about the activity?**

---

- He broke my feature....insisting it was too harsh.
- It wasn't challenging because my teammates were not encouraged to review each other's work and therefore there was no chance they would catch my additions.
- Looking silly about our lack of experience.
- Nothing in particular
- I was the insider threat, but I felt like I didn't really know what to do to be a threat to my team for the activity. Maybe just more suggestions to the insiders on things they should try to do.
- The first portion of the activity seemed like busy work, as there wasn't anything new being done in the activity. Creating threat models and misuse/abuse cases isn't anything new.
- I was taken by surprised that I was chosen to be one of the "insiders" and didn't quite know how to proceed
- it was very poorly executed
- Nothing
- The thing where the guy was bad.
- The deceit
- Presenting
- I was so caught off guard by threats within my group.
- That it was due at the same time as another large assignment

- Nothing
- Doing work.
- I didn't see it coming
- It took two classes to do a vast amount of work, which was to teach one thing (that inside threats are real).
- none
- The amount of time spent on the activity seemed disproportionate to the benefit of the ensuing discussion
- N.A.
- Trying to coordinate a single threat model with five different people.
- A lot of time spent to design a system - we do that often.
- The mole in the end won.
- N/A
- Requirements were ambiguous at times - MSFT Threat Modeling Tool has some issues that we didn't understand.
- Seemed like a lot of work and time just to introduce a topic.
- Our team's mole didn't show up to class
- the actual problem statement for the design was very simple
- Using the Microsoft Threat Modeling tool. Practical use for this seems minimal.
- The key member for this activity was not present in class. So our group was not impacted
- The Microsoft Threat Modeling Tool is not fun to work with.
- Putting a lot of work into the activity to not present it or turn it in.
- It wasn't incredibly informative
- It didn't feel like the activity had a point before the surprise.
- Sometimes it is kind of vague.
- The fact we didn't really experience it: our mole wasn't present aside from day 1, so no mole-like behavior was in the activity.
- I thought it was a good activity so nothing
- No
- MY team had really no idea how to model the system and it would have been a much better activity with more instruction in that regards beforehand.
- Working in a group. Group work for activities is tedious. I can finish the activity far quicker on my own.
- The typos and wording of this survey.
- Nothing
- Groups too large - we split off into abuse/misuse and the threat tool at one point, so we weren't able to actually see the affects of the mole
- Seemed like a lot of work in a short amount of time, and our abuse and misuse cases are not even graded for completion, making them pointless.
- Using Microsoft Threat Modeling. Completely useless.
- Had to do work.
- It was frustrating to work with an insider on my team.
- It was all pretty new (the tool and concepts) so the learning curve was pretty high, especially not

having worked with enterprise-level web systems before.

- Using the Threat Modeling tool can only allow the one person to edit it at a time and is local. If it just happens that your insider is the person with the tool they can change a lot of small things with no one in the group considering it an option.
- I thought it was pretty good all around
- There was a bit of confusion about some of the messages in the threat modeling tool.

**16 users did not answer**

## **10. What was the most useful concept you learned in the activity?**

---

- Don't be afraid to point out when something doesn't sound right.
- Code inspections are very important.
- Only give out degrees of trust. Do not trust anyone completely.
- Might seem silly, but the first hand experience of having someone betray the team, even on an insignificant level, leaves an impression that the same could actually happen in the real world.
- That there can always be an insider threat, even when you least expect one
- that insider threats exist
- To be aware of insider threats
- Not to trust my team
- How to tell if guys are bad.
- Don't trust anyone
- Be careful when you do hack/steal.
- Anybody can be a threat.
- Information about what consequences insider threats can have
- Distrusting your co-workers when their moods are sour
- How easy it is for a company to fall victim to an insider threat.
- Anyone can be an insider threat or dangerous at any time or on any team you are apart of
- Insider threats are real.... but perhaps in this context impossible to see because there are usually one or two tells (frustration, about to be fired, etc..)
- The most useful concept was the importance of frequent code reviews and not trusting the work of any one individual.
- To not trust the people I am working with.
- Trust no one, even your team members can be jerk faces
- Don't trust everybody.
- How easy it is to assume good intentions of colleagues, showing how easy insider threats can be undiscovered until it's too late.
- Being continually consciously aware of all possible security threats, for not all risks lie within the implementation.
- Insider Threats, are a thing, be careful.
- Insider threat
- Everything should be double checked by someone.

- dont trust anyone
- Simplicity
- No one should be above suspicion.
- Be wary and stick to good design principles you've learned
- Always double check other people's work.
- DON'T TRUST ANYONE
- Insider threats
- SQL Injection
- Don't inherently trust everyone
- How the prevent and detect
- To be vigilant.
- Double check your teammates' work
- Don't trust 1 person to not become corrupt.
- All cases of insider threat
- Seeing others' diagrams.
- Always be suspicious of developers and check over others work.
- Didn't learn any new concepts, just applied what we learned in class to the design process.
- Never trust anyone.
- Sometimes, just because a person is smart doesn't mean they're right. You should always think about something before you agree that it's a good idea
- I learned that the connections between objects are just as important as the objects themselves.
- Question everything
- How easily a mole can hide

**20 users did not answer**

## **11. What would you change about the activity?**

---

- Maybe select insiders via email with instructions.
- Each group should be encouraged to perform a "code inspection" or review of all their members' design work, to make it just a little more difficult for the insider threat and to give the other team members a chance to catch them.
- Try to create the insider threat outside of class so that the professor doesn't have to take them out to let them know what is going on. A really observant person might notice and figure out the activity.
- Combine it with some other lesson. Teach the first lesson during the first portion so the activity seems initially worthwhile. Not sure what you would mix it with though, abuse/misuse are taught too early in the semester and threat models hold enough weight to necessitate being taught in their own activity.
- Give more notice to insiders
- better direction for insiders
- Nothing.
- More bad guys.



- Nothing
- The ability to find your own case study so it'll bring creativeness
- Nothing.
- Focus more on specific incidents
- nothing
- Don't know.
- Nothing
- It was well structured already.
- Make it last only one period
- I would make 'planting' the insider threats more discrete.
- Nothing I can think of.
- I would make it simpler so it took less time to reach discussion
- If I could change one thing about the activity, it would be to give the "insiders" a more in-depth explanation of what they're supposed to be doing. As an "insider", I was unsure of how to properly compromise the system. If I had a better explanation of what to do, I might have been able to do more to the system.
- Make it an even more drawn out activity, maybe work into the case study before the first deliverable is due.
- Reduce design activity, such as by not doing the requirements.
- Nothing.
- Not much.
- More rigorous Threat Modeling practice
- Shorten it.
- make the problem more challenging to design
- Maybe 2 moles in case 1 of them doesn't come in.
- Find a better tool than the Microsoft Threat Modeling Tool.
- Probably do it before Spring Break so senioritis doesn't kick in.
- Use something else other than the microsoft threat modeling tool
- Make it a new topic or more of a spin on a topic to make it feel less repetitive beforehand.
- None
- Nothing
- No
- I would have a tutorial or example diagram that we go over beforehand.
- Do a little bit more with Microsoft threat modeling tool before hand
- This survey.
- Nothing
- View more team results
- Smaller groups. Encourage collaboration on the threat tool
- Remove the supporting document, make it just the threat model.
- Not using Microsoft software.
- Nothing.
- Nothing; I thought it was great.

- Not use the Threat Modeling tool
- More emphasis on the threat model as that is what we presented in class
- Possibly provide more specific or detailed instructions to moles. I felt as though ours did not really do much.

**19 users did not answer**

## **12. Any other comments you would like to activity?**

---

- What?
- It was fun
- Any other comments you would like to activity?  
like to activity?  
to activity  
?
- None
- Guys are bad
- Nope
- NA
- I don't know how to activity a comment, but no.
- No
- nah
- Lets Go Duke!!!
- Nope
- Nope.
- I think this is an activity that should be done again for future classes.
- no.
- I enjoyed the concept very much.
- "Any other comments you would like to activity?"  
What?
- Was a great learning experience for the amount of security deterioration an insider threat can impose on a system.
- Again, easy simple, proved a point. (Question 13 on this survey is empty)
- Overall, great activity. Need clearer requirements and more rigorous Threat Modeling instructions
- Even though it was applying all the concepts we learned previously in the course, the activity felt a little redundant like we had done it already.
- It was fine
- It's definitely better if the mole is actually there.
- None
- No
- It would be great getting external experience from security experts
- Make this a more important project that people take more seriously so it sucks more when they find there was a mole. Drives the point more.

- How do I activity a comment?
- Nope
- I was a great idea.

**38 users did not answer**

**13.**

---

--	--	--	--	--

Copyright © 2015 [Rochester Institute of Technology](#). All Rights Reserved. | [Disclaimer](#) | [Copyright Infringement](#)