**Risk Management Case Studies (CIS 411)**

**Case Study #1**

Name: Chad Ballay

Date: 5/3/2020

***Directions:***

*After viewing Case Study #1 in Week 1, please complete the worksheet below. Be sure to answer each question completely.*

*Think of your current audio/visual/stereo system. Your system could include a television, media player, stereo system, and game console. (If you don’t currently have one, think of one you’ve had or a relative has had). Use the process below to develop a risk analysis for it.*

1. **Asset value**

*Select the answer that best fits your current audio/visual/stereo equipment. Questions 1-4 are multiple choice. Please bold or highlight your answer.*

* 1. Is it old or new?
     1. New
     2. **1 – 2 years old**
     3. 3 – 5 years old
     4. 6 – 9 years old
     5. Over 10 years old
  2. What shape is it in?
     1. Excellent
     2. **Good**
     3. Fair
     4. Poor
  3. How long have you had it?
     1. 1 year or less
     2. **1 – 3 years**
     3. 4 – 6 years
     4. Over 7 years
  4. Who uses it (check all that applies)?
     1. Me
     2. My spouse / partner
     3. **Other family**

1. **Threats**

*Answer questions 1-2 by typing your complete answers.*

* 1. There are four main types of threats: **Environmental, Man-made, Abuse vs. Misuse,** and **Mechanical.** What are the threats to your equipment? List at least four specific threats from each of the categories above.
     + 1. My son has some temper issues with Fortnite and xbox controllers…. Recent experience that I wasn’t aware was going to be an issue till last week’s tantrum.
       2. I live nearish tornado alley so risk of weather events. Surges to power or just plain storm damage.
       3. My youngest doesn’t understand how to safely interact with them but also isn’t prevented very thoroughly. She has put dvd’s in upside down as well as tried climbing some of the shelving.
       4. The design of my entertainment system puts a premium on hiding the electronics instead of having optimum airflow so overheating has occurred.
  2. What is the likelihood of each threat impacting your equipment (in %)?
     1. Should now be 0 but that’s due to communicating to him the penalty if I catch him throwing a controller down again. Nothing is actually stopping him beyond his own awareness of the impact.
     2. It hasn’t happened to this generation of hardware I have so also pretty low. The hardware will fail for other reasons it seems.
     3. She’s already decreased the value but not the functionality by defacing things with markers. So that’s a 100%. She hasn’t broken functionality yet so if impact is defined on loss of functionality I’ll round that one down to a 25% chance. She’s two and is really not aware of how to use the dvd player and tv correctly.
     4. Awareness due to past learned lessons has this already being mitigated going forward. Installed a low powered fan and keep the cabinet open while in use. So historically it was a 100% since I learned that the hard way. Going forward I would put it at 10% since somehow someone will forget to leave it open while running.

1. **Vulnerabilities**

*Answer questions 1-2 by typing your complete answers.*

* 1. Where, when, and how is your equipment vulnerable?

1. Where: My home is not Fort Knox. Several large windows look into the living room so a smash and grab would be very feasible. I also live in a wooded lot so trees could smash it. I also have the equipment at floor level in the open so access isn’t a problem for anyone. Kids, dogs, thieves, backed up sewage, etc…
2. When: Both myself, the wife, and our kids are away from the house for extended times during the day and with a consistency that can be planned for. From 8am till the afternoon is the likely best time. We don’t often eat in that room but meals or snacks during usage are a threat.
3. How: I live far enough away from my neighbors that they wouldn’t notice an intruder. The kids are allowed to use it since this is their house too and any bit of self-sufficiency is boon to my ability to get all the things done that I need to do.
   1. List at least five ways in which your equipment is vulnerable to the threats:

* Theives can steal it.
* My dog could decide that some part of it is a chew toy.
* I could forget to leave the cabinets open when using it so it can overheat.
* A nearby lightning strike could overwhelm my surge protector.
* I try not to pre-emptively ban the kids from using something so they have the chance to inevitably break it. No prevention there, just a response going forward.

1. **Impact**

*Answer question 1 by typing your complete answers.*

* 1. What’s the impact if your equipment is compromised (Monetary, Inconvenience, etc.)?

Long ago I would just list off the depreciating value of the goods + the man hours it would take to file the insurance claim + the cost of my deductible and call it done. A few days without a tv/dvd/xbox would be a minor inconvenience…. Now with so much PII, PCI, and even HIPAA data being on modern electronics things are at a higher level. I’ve got to change logins and possibly cancel accounts for some of the services. Did my kids save contact info for themselves or friends? Do I have accounts to media sharing sites for family photos that are now at risk? Etc, etc….

1. **Controls**

*Answer questions 1-2 by typing your complete answers.*

* 1. What controls are in place to protect your equipment? (Consider the broad categories of technologies, process, policy, awareness, infrastructure, etc.)

I now have a reloadable credit card that I use that covers my reoccurring subscriptions like this. So if it gets misused it only affects a very limited portion of my finances.

I’ve installed a low power fan to help with the airflow but I need to wire up a temperature sensor as opposed to just a manual toggle switch.

I’ve had age appropriate discussions with the kids about the cost/value/impact of the equipment to try and get them to actively help with this task.

Bought a monster of a surge protector since it was a one time cost that didn’t require anything beyond the initial setup but would give me ongoing protection.

The family puts the burden of modifying and fixing anything related to it on me so that there is no chance of cross purposes or understandings on what’s the appropriate setup.

While not exclusively for this reason, I’ve always made sure to have a pet dog. My dog isn’t going to stop a dedicated intruder but they are yappy enough to discourage an opportunistic thief.

I try to maintain a decent enough list of what accounts are enabled on what devices. At first just due to adopting non-trivial passwords as a practice. Typing a 16 char long password that looks like gibberish using a TV remote to use an onscreen keyboard goes a long way to limiting the number of services I setup.

* 1. How often is each of the controls used?

Most of them are always used. I’ve learned the hard way that I won’t be able to enforce an inconsistent schedule for processes. Either it has to be automated or built into the standard operating procedures else over time it’ll be abandoned. For instance, overbuying on a surge protector rather than unplugging equipment to avoid power surges. Or taking the time to have a quiet fan always running rather than just remembering to leave the cabinet door open. Or having a dog that barks as a pet instead of getting a more laid back pet.

1. **Risk Mitigation**

*Answer questions 1-2 by typing your complete answers.*

* 1. How do you reduce the risks to your equipment?

Over buy on protective measures like surge protectors. Over communicate to kids to be careful. Keep lines of sight in my yard as clear as I can tolerate so criminals aren’t comfortable on being unseen. Maintain a punchlist of serial numbers, purchase information, insurance information, and a healthy emergency fund. Not just for this but as a matter of practice.

* 1. Have you purchased anything or taken other steps to reduce your risks?

Surge protectors and fans. An occasional extended service warranty. I live in the south and in a suburb so I’m not sure if a shotgun is just a birthright or an actual purchase for risk reduction.

**Change the scenario to the following:**

*Answer question 1 by typing your complete answer.*

1. Your stereo system set up is a high-end brand such as Revel or B&W. How do your answers change?

Documenting the purchases and increasing my insurance coverage would be the main change. I could also try to offset the purchases of the components so that the lifecycle for them are spaced out better. This way the financials are levelized more.

I can’t do much more with the kids. They understand as much as they can for their age and I really can’t live in a prison so the risk they pose can’t be reduced much more. Maybe invest more in giving them better tablets/phones so they are less likely to use the upgraded set?

Same with the environmental aspects. It would take a lot to tackle rearchitecting the furniture. Structurly the house can’t be made more “bad weather” proof. Same with the features to discourage thieves. I feel I’m at the elbow in the J curve where diminishing returns just eat into the effort too much. Maybe install a home security camera system but that shifts the risk from physical thieves stealing my equipment to now having to worry about who can see into my home.

Maybe I could look at creating separate and device specific accounts for services. Probably talk more with the kids on information security. But those might be more than I can realistically do above what I’m already doing.