Desmond Hughes

Purdue University Global

IT286 Network Security Concepts

Howard Weinraub

March 27th , 2023

For the risk assessment there are the acronyms SLE, ARO, and ALE. SLE means Single Loss Expectancy, which is money that you are expected to lose. ARO means Annualized rate of Occurrence, which is the risk turning real expresses in percentages. ALE means Annual Loss Expectancy, determines if the risk will be real in a year. Putting the acronyms together can even be made up to make up another, for example SLE \* ARO = ALE

The five actions you can do to reduce risk:

* Being Educate on the best security practices.
* Having secure hardware.
* Making sure your employees are educated.
* Contingency plan.
* Have an insurance policy that is comprehensive with cyber and technology.

Staying on task can help reduce the risk by not going on to inappropriate or non-work-related websites that can trace or infect your computer with viruses. It will also be positive in a group setting by others knowing that they can count on you to stay on task and not goof off or get distracted by another thing. Meeting deadlines will help reduce the risk by making the turn in date because the longer you wait and hold things off the more likely others can access it. This can also promote a positive group setting by making the team run smoothly and making sure that everything is going as it should. Utilizing feedback can have a positive impact by fixing the problems and enhancing the thing the feedback talks about or discusses, so that the next time something can be done more efficient or better. Utilizing feedback can also be positive in a group setting by help building the team closer together so that they know what needs to be work on so that the next time everything runs smoothly.

There are many risks that come when people associate with cloud computing and virtualization. Some reasons are reducing visibility and control, it can be compromised, increased complexity, When deleting data, it may not completely delete it and stored data being lost. Customers and user of cloud computing can lose visibility and control over some of their assets and data, this is really based on the cloud service model and how it is ran and monitored. Some of the cloud storage can be vulnerable which can lead to a compromised. With APIs being accessible and compromised they can be exposed. Another risk and problem are the data not being completely deleted. With the data being in the cloud storage and spread across networks and storages it may sometimes be hard to fully delete the data. Another risk to add to the following is that the data and credentials can be stolen as well. Gaining access to a user’s cloud the hacker can also gain access to the CSP to acquire additional resources from the user. Another risk is it can increase the complexity for users and customers of the cloud. The complexity could leave security gaps due to following policies or methods. One more risk is that the data stored can be lost. Data might be accidentally deleted by the provider. Losing the encrypt key can be another reason the data can be lost. It doesn’t just have to be hackers or cyber-attacks.

|  |  |  |
| --- | --- | --- |
| Five Key Areas | Where does it match? | Where can it be improved? |
| Cookies being used sent to the browser to be stored | Under the Cookies subtitle | Use Google Analytics and other third parties to content visitors |
| Will not share personal information to third parties | Under the ‘Sharing Your Information” subtitle | I think this is good enough |
| Collects personal information when you register | 1st paragraph under information Collected by Accion and How We Use It Subtitle | It is only used when you voluntarily provide it to the website, |
| Collects IP addresses and domain names | 2nd paragraph under information Collected by Accion and How We Use It Subtitle | Help with your subscription preferences |
| Ask to complete surveys for research purposes | 3rd paragraph under information Collected by Accion and How We Use It Subtitle | Send it periodically |
| Use the information to inform you about new products. | Opt-Out | Receive only specific communications or none at all |

Bradley Manning is facing over hundred years of prison, after putting the US and the friends of the US, in danger over the world. There was a video of a helicopter that killed multiple people, and they think Manning is behind it. Some people called Manning a traitor. It is also said no one has sympathy for him of no kind, because he violated an oath from the Army. After finding out Manning did it, it took a tole on a number of government agencies. Manning was aiding the enemy in attacking.

Reliability is completing tasks on time and when you complete those tasks make sure that it is quality work. It also can be Showing up to work on time, making sure business is handled when there is a problem, and making sure deadlines are meant. Being reliable is being considered someone you can count on. This is important during a risk, because you can depend on this person doing the right thing. Accountability in a workplace is having responsibility for your own action and the way you perform and make decisions. Accountability worker sets clears expectations and can be mature in situations. Accountability during a risk is very beneficial, because the person would follow through until the problem is taken care of and fixed, he will also communicate the situation clear and forward with the ones around him. Timeliness in a workplace is someone that keeps up with time and arrives and complete things on time or even early. To do that they understand the requirements, and keeps up with deadlines. They also plan out how they would complete or finish a project. During a risk being timeliness would be helpful, because they would handle this in a timely manner, and prioritize it.

Diagram, schematic

Description automatically generated

Threat is a circumstance which can conclude something that is unauthorized, destructive, disclosures, or even information that has been changed. Vulnerability is the weakness in the information system or something that can be exposed and defenseless by a source. The difference between the two is that the vulnerability can lead to the threat becoming a threat. How it starts is somewhere in the data it gets exposed, and the hacker or virus slips through the cracks and becomes a threat to the user.

References

*Bradley Manning: Whistleblower or traitor?* (2013) *NPR*. NPR. Available at: https://www.npr.org/templates/story/story.php?storyId=208259660 (Accessed: March 28, 2023).

*Guide for Conducting Risk Assessments - NIST* (no date). Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed: March 28, 2023).

Messer, P. (2020) *Risks with cloud computing and virtualization - comptia security+ sy0-401: 2.1*, *Professor Messer IT Certification Training Courses*. Available at: https://www.professormesser.com/security-plus/sy0-401/risks-with-cloud-computing-and-virtualization/ (Accessed: March 28, 2023).

Morrow, T. (2018) *12 risks, threats, & vulnerabilities in moving to the cloud*, *SEI Blog*. Available at: https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/ (Accessed: March 28, 2023).

National Institute of Standards and Technology. (2012, September). Guide for conducting risk assessments. NIST Special Publication 800-30. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (n.d.). http://csrc.nist.gov/