Chris Fullerton

Week 4 ethics and law reflection

Summarizing the NIST and why minimum necessary matters is important for many reasons including privacy protection, risk reduction, compliance and ethical responsibility. NIST is the National Institute of Standards and Technology, a U.S. federal agency under the department of commerce that plays a role in the cybersecurity framework and guidelines. NIST breaks down the incident response into four phases. The first phase of the incident response is Preparation. Preparation builds policies and response teams to be prepared for attacks. They prepare by training and setting baselines into reducing risks. Phase two is the detection and analysis phase. This is where they will use alerts, logs, and reports to detect and analyze attacks. They validate incidents impacts through the CIA (confidentiality, integrity, availability). Phase 3 is the containment, eradication, and recovery phase. Like it sounds this phase will contain incidents and stop or delete attacks or corrupted files and data. This phase will also use the recovery to restore systems and operations back to normal. With the prep and training recovery can be a smoother process. Phase four is the post incident activity. This is almost like the preparation phase but when an incident happens everything is recorded and then studied. This is the learning from mistakes phase where patch gaps and improvements come from. The Minimum Necessary principle is incredibly important in NIST incident handling because this will reduce the amount of important information from getting leaked. The minimum necessary principle is only access, use, or disclose the minimum amount of information needed to perform a job duty. This works by not over sharing so unnecessary important information doesn't get leaked. Many laws are in place so information doesn't get leaked and used for things like blackmail. These laws can have heavy penalties causing a ton of legal trouble. If the minimum information is used then the less chances of running into unnecessary laws being broken. This also reduces risk reduction and increases privacy protection. With NIST guidelines and the Minimum Necessary Principle in place the risk of being out of compliance and in the legal guidelines will keep businesses and people safe when sharing important information.

How to apply it

Let's say a faculty member is suspected of getting sensitive information from the universities network using a personal device and the IT security team is tasked to investigate. These items to capture are the why and justification of the data gathering. The team would need to show login times access attempts the file transfers and the justification would be are they within scope of the consent when agreeing to IT policies using the universities network. The reason not to avoid it is the personal device contains private, non work data that is personal information. This could cause legal issues getting on the faculty members device if the suspicion exists.

Muddiest point

I would still be confused on how far you could investigate a situation like this. How would you know if you could get into a faculty member's device if they are suspected of a crime. What would be the right legal action?

Portfolio Notes

SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | CSRC

Chat gpt sage use.