Chris Fullerton

Week 5 Reflection ethics and law

This week I learned about Governance, risk and compliance and why it's important for ROE (rules of engagement). This boils down into 4 major parts, Policy, Standard, Procedure, and Guideline. Policy can be described as the what and why as in the what being hocking college policy and the why being the authorization and access agreements. Standard is the must do's as in detect and protect. Procedure is the how to idea that tells you how to do procedures and who to contact in case of incidents. Guidelines are the should do's, it offers flexibility in the procedures. There is also the Accountability Mechanisms, Owner, Approvers, Review Cadence, and Enforcement. Owner is the system owner who approves the in scope system along with instructors and students that test in the ROE boundaries. The approvers are Program directors and network owners who provide authorization. Review Cadence is the ROE reviewed before each test or exercise for annual policy alignment. Enforcement would be disciplinary or legal action from violations.

Course eBook (e.g., Security Awareness, Ethics & Law): Emphasizes that security actions must be **authorized, ethical, and accountable**. ROEs directly operationalize these lessons — e.g., "unauthorized testing" is not just unethical, it's a violation of law (CFAA, GDPR, HIPAA).

Two ROE clauses I think are important are the Data Handling and retention, and the Explicit Authorization clause. The Data handling and retention clause I think is important because when collecting data under a ROE you need to be careful not to get any sensitive or personal information. You could possibly break laws like HIPPA. With explicit Authorization

clauses you could accidently go out of network or out of scope and violate code of conduct and applicable laws.

My muddiest point this week would be in the Deconfliction. Mostly with scheduling, how would business go about moving employees in the IT around to make sure tests are being conducted at the correct times. This gets muddy to me because I've worked a lot and it seems like it would become hard with an employer that runs 3 shifts or 24 hours a day.

What I would add to my site is a good guideline on ROE and governance, risk, and compliance. I think it’s important to understand the implications of going out of scope or see how easy it would be to accidentally gather wrong or sensitive information. To know how to avoid such incidents and whom to contact in case one does go out of scope would be important.

Used sage as a guide