Contracts Use Cases and Risk

Kevin Lanning, CISO

University of North Carolina at Chapel Hill

Challenges of the Past

- Prior to 2005, small information security teams.
- Risks were sometimes only discovered when an incident occurred.
- Contracts were reviewed by staff not trained in risk assessment.

Engaging to Control Risks

- UNC-Chapel Hill established Information Security Liaisons via policy.
  - Every department must have a liaison and a backup.
  - Provides local context.
- Developed questionnaire for Purchasing.
- Integration with ERP software ideal.
- If purchases below a set amount don’t go through Purchasing, maybe legal?
- Purchases or contracts that involve sensitive information must have a risk assessment by policy.
- Maintaining trust through focus on mission.

Risk Assessments

- Many tools and risk assessment management frameworks (ISO 27005, NIST 800-37).
- The Information Security team usually conducts.
  - Developed our own tools with spreadsheets and survey tools.
  - Questions vary with relevant regulation, standards, etc.
  - We assess the controls in place against our policies and standards.
  - Suggest compensating controls.
- We have firms available that were selected from RFP if we are busy or if we don’t have the right skill set.

Risk Assessment Evolution

- With an increase in requests to purchase cloud-based products, we are assessing risks more based on interviews and written descriptions of controls than on traditional interviews.
  - Cloud controls matrix plus SOC 2?
  - Leveraging a document prepared for Payment Card Industry and/or other types of compliance?
- Controlling risks more based on contract terms.

Risk Acceptance

- Risk treatments from which to choose:
  - Avoid-choose not to purchase.
  - Transfer-transfer the risk via contract.
  - Modify the risk-limit a service to intranet.
  - Accept-If the cost of mitigating controls are too high and/or the likelihood and/or impact of successful exploit are low, leadership may choose to accept the risk.
- Take the risks back to the business owners and data stewards.
- Plan of Action and Milestones (POA&M) to follow progress on gaps.
- Annual support payment can be a natural time for quick check-in or to raise the bar given new threats.

What Might Not be Risk Assessed?

- Imagine a company offers “free” software that deals with sensitive information.
  - Will your procurement systems see the arrival?
  - Will your legal department see it?
- Employees with credit cards sponsored by their employer:
  - Would a small purchase of a product that works with sensitive information be detected?
  - Imagine an employee pays a monthly fee via the card for creation of online forms that collect sensitive information and email that information to central IT systems.
- ISLs can be very helpful-Trust for a positive dialog about risk.