1. Target: CSuite (CEO,CIO,CFO) at a company of ~200 People
   1. Company Cybersecurity Risk Assessment
      1. Assessing Technological Endpoints
         1. Importance of identifying data and how its protected/managed.
         2. Determining the role of each technical branch at a company
         3. How to ask the right questions to the technical leads about what information + data is exposed to the public and why
      2. Understanding the Function of Proper IT
         1. Distinguishing the differences between the various forms of IT structures (In-House, Domestic Outsourcing, Foreign Outsourcing)
         2. Identifying the key roles in IT infrastructure
         3. The Dangers/Benefits of outsourcing IT for Security
      3. Employee Facilitated Risk
         1. Identifying employee training with respect to information security
         2. Frequency of employee related attacks
         3. Internal data theft, employee network access, determining who knows this information
      4. [Consequences](https://www.exed.hbs.edu/risk-management-corporate-leaders/)
         1. Loss of Competition
         2. Lawsuits
         3. Brand Damage
         4. Unethical Practices
         5. Geopolitical Crises
         6. Pure Financial Loss
   2. Policy Creation
      1. Separation of Data Systems
         1. Locating SMEs (Subject Matter Experts)and identifying skill sets
         2. Identifying data categorizations (Personal, Company, Public)
         3. Establish ownership of data categories to different professionals based on SME status
      2. Developing Data Policies
         1. Drafting data management policies with finance leads, budgeting leads, and the leads of each data section
         2. Identifying risk tolerance with company financial and analytical experts with respect to each data section
         3. Validating Risk against company values and ethics
      3. Implementing Data Policies
         1. Facilitating specified company training programs to match data classifications
         2. Onboarding managers over technical leads on policies in data integrity
         3. Establishing a concrete internal policy auditing system with corporate leads
   3. Types of Attacks
      1. Social
         1. Phishing
         2. Spearphishing
         3. Tailgating (Physical Component)
      2. Ransomware
         1. Forced System Lock-out
         2. Data Compromise
         3. Personal Data Extortion
      3. Malware/Viruses
         1. System Espionage
         2. Developer Cycle Downtime
         3. Loss of Critical Data, Theft of Critical Data
      4. Extortion
         1. Whaling (CEO Fraud using stolen personal data)
         2. Employee Personal Attacks
         3. Honey Trapping
         4. Deepfake
      5. Physical/Infrastructure
         1. Summarized in [this video](https://www.youtube.com/watch?v=JsVtHqICeKE)
   4. Mitigation
      1. Elements of an incident plan
      2. Enforcement of Data Policies
         1. Awareness of the hierarchy of data ownership
         2. Frequent auditing of the policy implementations
         3. Maintaining hierarchy through employee transitions
      3. Preserving Data Integrity
         1. Frequent system backups
         2. Facilitating testing engineers who can build large test systems
         3. Logging everything of relevance
      4. Continuous and Extensive Training
         1. Internal courses with proprietary knowledge
         2. Conferences, workshops, third party support
         3. Company rules and guidelines with incentives
      5. Proper Insurance Plans
         1. Designating professionals to handle when things go wrong
         2. Adequate policies for scaling company sizes
         3. Establishing policy for notifying stakeholders
   5. Exercises
      1. Have the CXX determine what current data policies are in place at their own company, who is in charge of those, and facilitate a discussion on which may be antiquated and in need of removal, and which may need to be created to suit the needs of the company.
      2. Provide a sample list of questions the CXX can ask their subordinates, particularly leads of departments, in order to gather information on the security health of their company.
      3. Encourage **Proactive** over **Reactive** cyber risk, by providing a list of real world cases where a lack of integrated data policies led to massive financial loss. (Sony, Facebook, etc..)
      4. Discuss with the CXX their expectations of company scaling and the types of people in their organization capable of hiring the type of people to meet these demands
      5. Have the CXX request a physical audit of their perimeters by Physical Pentesters to see how their infrastructure safety is in its current state
      6. Have the CXX identify the leaders of IT infrastructure at their organization. The CXX should request the IT leaders to develop lists of who has access to what security features at the company and ensure it follows a top down approach (Principle of Least Privilege).
      7. Determine how much, if any, the CXX’s finance department has reported in losses due to Cyber-attacks. Evaluate this with respect to the current provisions for training and security-related employment.
2. Target: Non-Technical Management over Technical People
   1. Introduction to Cybersecurity Risk
      1. Basic Introduction to types and methods of attacks - High Level
         1. Web Application Exploitation
         2. Database Manipulation
         3. Social Engineering
         4. Supply Chain Exploitation
         5. Application Exploitation
         6. Cyber-racketeering Schemes
      2. Famous Cybersecurity Attacks
         1. Recent - Solarwinds
         2. Recent - Microsoft Exchange
         3. Recent - Facebook Password Breach
         4. Recent - WannaCry
         5. Old School - ILOVEYOU
      3. The Role of the Manager
         1. Hiring Requirements
         2. Maintaining Quality of Standards
         3. The Importance of Dev-Ops and Code Structure
         4. Sufficient Staffing
         5. Diversity of Ability
   2. Determining Appropriate Risk
      1. Evaluation of the Cost of Appropriate Staffing
         1. Penetration Tester - Cost and Skillset
         2. Reverse Engineer - Cost and Skillset
         3. Fuzz Tester - Cost and Skillset
         4. NetSec Engineer - Cost and Skillset
         5. IT Services and Protection - Cost and Skillset
      2. Calculating Implied Risk
         1. Identifying Sources of Risk in a System and Organization
         2. Data Integrity
         3. Predicted Incident Reporting
         4. Identifying Historical Cost with Respect to Security Incidents
         5. Ethics of Reporting and Evaluation of Risk factors
      3. Comparing Staffing Cost with Implied Risk
         1. Identifying Staff Scaling with Respect to System Size
         2. The Financial Benefits of Proactive instead of Reactive Security
         3. Securing Customer Trust with Strong Security
         4. Calculating Expected Incident Cost against Staffing Costs
         5. Cybersecurity Related Insurance
   3. The Importance of Proper Training
      1. Understanding Valuable Certificates
         1. OSCP - Offensive Security Certified Professional (The Ethical Hacker’s best friends)
         2. CompTIA, A+, Security+ - IT Networking + Security
         3. SANS certifications - All over the Board
         4. AWS Security Certificates
         5. Azure Security Certificates
      2. Conferences Worth the Investment
         1. Blackhat Conference
         2. DEFCON Conference
         3. Human Hacking Conference
         4. RSA Conference
         5. SANS Conference
      3. Encouraging Learning Growth
         1. The Importance of Continual Study
         2. Written Resources - No Starch Press, O’Reily
         3. Humble Bundle Cyber Security Bundles
         4. Open Source Exercises - CTF, HackTheBox, TryHackMe
         5. Video Resources - LiveOverflow

**Introductory Sampler**

**Sample Questions from Section 1:**

1. Your company is in charge of several distributed web applications built on AWS infrastructure. You do not run any of your own networking, and all of your engineers develop directly through Amazon’s environment, or on systems that are tightly networked. What form of Cybersecurity attack is your company the most susceptible to?  
   Web Application Exploitation
2. You run a small company in the Midwest that specializes in the design and development of drill bits for manufacturing corporations. You have very little software related systems other than CAD software that runs on a local network, and a publicly available Microsoft Exchange server. A salesman schedules an appointment to meet with your CIO to discuss his company’s Ransomware protection software. After your CIO declines to purchase said software, a week later, all of your systems are compromised by the same type of attack the salesman discussed with the CIO. Your company has likely fallen prey to what kind of attack?

Cyber Racketeering Scheme

1. Briefly Describe the Solarwinds Attack  
   Solarwinds was a supply-chain exploitation attack conducted by nation-state hackers. The hackers gained control of the update pipeline for popular network monitoring software, Orion, and used it to inject malicious code into corporate and government networks to analyze Network Traffic
2. Provide Three Reasons for having Security related Dev-Ops in Place
   1. It facilitates common-sense maintainability in large systems
   2. It automates the detection of discovered vulnerabilities
   3. It aids in the prevention of regression issues

**Sample Questions from Section 2:**

1. Your company is looking to hire an individual with a large amount of experience in breaking into Web Applications and finding vulnerabilities related to public facing software interfaces. They want an individual capable of producing short term scripts to enable them to break into company software infrastructure using only what the public has access to. What type of security professional should they hire?  
   A Pen-tester
2. In the past 5 years, your company has suffered 2 major data breaches, 5 minor database leaks, and some private information has been leaked 10 times. The risk analysis statisticians have determined that your company spends an average of $100,000 dollars per major data breach, $5,000 per minor data breach, and $1,000 per private information leak. What is the average amount of money your company spends a year on security incidents total?  
   Major Breaches: $100,000 \* 2 = $200,000

Minor Breaches: $5,000 \* 5 = $25,000

Private Breaches: $1,000 \* 10 = $10,000

Total Cost = $235,000

Average Yearly Cost = $235,000 / 5 = $47,000 a year

1. Your company reportedly drains $100,000 a year paying off Ransomware attacks that affect their network. Your analysts have determined that hiring a Network Security professional will reduce the number of Ransomware attacks to one out of every 11 years. How much money will you save/lose by hiring a Network Security professional at 80k for a ten-year period (assuming no raises, changes in the amount paid to the ransomware attack).

Engineer Cost for 10 years: -$80,000 x 10 = $800,000

Money Saved not being Attacked for 10 of the 11 years: $100,000 x 10 = $1,000,000

Cost of Ransomware on the 10th year = -$100,000

Total Money: $1,000,000 - $100,000 - $800,000 = $100,000 over 11 years

**Sample Questions from Section 3:**

1. One of your employees is transitioning to become a Web Application Penetration Tester at the company. He/she has little experience in the field, but does know quite a bit of Bash and Python. What certificate training would you request to develop for his/her skill?  
   OSCP
2. You have an employee who is looking for some corporate level training on a very particular skill to help train their abilities in a very professional, corporate environment. You want them to attend lab sessions over several days on the topic. What conference should you offer to send them to?

Blackhat or DEFCON, there are multiple answers but these are definitely top of the list

1. Over the next year, your workplace is developing a program where employees can take every Friday off to study the topic of their choice, so long as they write a short presentation on the topic that they studied. If you have an employee who is interested in learning about IoT hardware hacking, what resources would you recommend them?

Ambiguous answer, likely the ‘Hacking the IoT’ guide just published by No Starch Press