**EMCS2430: Human Factors: People and Software**

Assignment: Develop & Evaluate a Good Defense

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

1. Review "Appendix D: Best Practices by Organizational Group" found in the recent CERT publication Common Sense Guide to Mitigating Insider Threats.Preview the document Which of these practices did you witness in the "The Company Man" film you viewed for the previous assignment? Which ones would you add?

**Used by the company in the Film**

*“Know and protect your critical assets.”*

The company definitely knew their critical assets, and they made efforts to protect them, but the efforts were not well organized.

*“Consider threats from insiders and business partners in enterprise-wide risk assessments.”*

The company definitely considered the threats posed by the Chinese company to be a threat to the entire organization.

**Not demonstrated in the film**

Clearly document and consistently enforce policies and controls.

Develop a formalized insider threat program.

Anticipate and manage negative issues in the work environment.

Be especially vigilant regarding social media.

Structure management and tasks to minimize insider stress and mistakes.

Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.

Implement strict password and account management policies and practices.

Institute stringent access controls and monitoring policies on privileged users.

Deploy solutions for monitoring employee actions and correlating information from multiple data sources.

Monitor and control remote access from all endpoints, including mobile devices.

Establish a baseline of normal behavior for both networks and employees.

Enforce separation of duties and least privilege.

Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

Institutionalize system change controls.

Implement secure backup and recovery processes.

Close the doors to unauthorized data exfiltration.

Develop a comprehensive employee termination procedure.

**Very important in my opinion**

Clearly document and consistently enforce policies and controls.

Develop a formalized insider threat program.

I only chose two because I think the exercise of

*2. Next, choose one of the following three cases from The CERT Guide to Insider Threats (Chapter 8). The cases are: Sabotage Case 8 (p.247), Theft of IP Case 5 (p.261-262), and Fraud Case 9 (p.267-268)*

*3. Look again at Appendix D in the Common Sense Guide for possible defense practices and explore what the guide has to say about those practices in more detail. For the case you selected, design a corporate defense approach (not a cyber algorithm specifically) that could have prevented, detected or mitigated against that case.*

So the scenario is all the code for a critical part of the business in one place, under the control of a single person and that person successfully argued that this was the best way to handle things. Seemed a like a set-up and indeed it was. Apparently the insider argued that having the critical infrastructure of the company under the control of one person was more secure. And, obviously this was wrong ( for many reason other than just security ). I am going to break this down into three phases for practical purposes :

1. How do you counter the argument of an employee who insists on being the sole person with access.