Assignment 1: Defining the cyber security environment.

Due Date: Sunday February 5, 2017

Class enrollment is 35 students. Form 7 groups of 5 students each

Resources: Many industry reports are available. To assist you, pointers to some recent reports are given below. I recommend that each student choose one report – each student in the group must choose a distinct report. The value of this exercise is to get an overall picture of the cyber security environment.

Objective: Learn and understand the cyber security threats and the challenges.

How: Review industry analysis reports – each student will choose a report to read and report. The group will then meet and develop a report that identifies commonalities and differences in approach in the various industry reports. Finally each group will prepare one report – 4 to 5 pages. At a minimum the reports will answer the following questions:

- What are the most significant threats treated
- How long does it take to detect compromise
- What is the remediation cost and time
- Time to get in: what are the different ways of compromising - How long are the bad guys in the system?

Class Presentation: Each team will present their results in the class on February 6. Each team will have 10 minutes. **Each team must practice their presentation twice before the class.** Each team must include the following statement on the first slide – "We have practiced the presentation two times". This will make class presentations more effective. If you do not practice, you will not be allowed to present in the class.

Pointers to recent industry reports

Verizon (DBIR) http://www.verizonenterprise.com/DBIR/2015/ **IBM (X Force)**

IBM X-Force Threat Intelligence Quarterly 2Q 2015 https://www-01.ibm.com/marketing/iwm/dre/signup?source=swg-

WW_Security_Organic&S_PKG=ov36741&S_TACT=C41303YW&dynform=19019
Security Incidents http://www-03.ibm.com/security/xforce/xfisi/

IBM 2015 Cyber Security Intelligence Index http://www-01.ibm.com/common/ssi/cgibin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03278 USEN&attachment=SEJ0327 8USEN.PDF

Ponemon http://www-03.ibm.com/security/data-breach/

Sophos

Vulnerabilities https://www.sophos.com/en-us/threat-center/threatanalyses/vulnerabilities/VET-000756.aspx

Threat Dash Board https://www.sophos.com/en-us/threat-center/threatmonitoring/threatdashboard.aspx

McAfee http://www.mcafee.com/us/resources/misc/infographic-threats-predictions-2015.pdf

Quarterly-threat http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf

CISCO **Cyber Risk Report** http://tools.cisco.com/security/center/cyberRiskReport.x?currentYear=2015&i=60 **Mandiant**

APT1: Exposing One of China's Cyber Espionage Units

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Symantec

2015 Internet Security Threat Report, Volume 20

https://www.symantec.com/security_response/publications/threatreport.jsp?inid=us_ghp_hero2_istr20

Assignment 2: How has the threat changed with time. (Note: Each student submits a separate report.)

Due Date: February 13, 2017

In Assignment 1 each student studied one report. In this assignment you are to collect reports from 2 previous years – from the same industry group. The goal is to get a feel for how the understanding of the cyber security environment changed.

Each student will submit a 2 page report.