BIRMINGHAM CITY
University

Cyber Security Incident Management

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

The Higher
Education
Academy

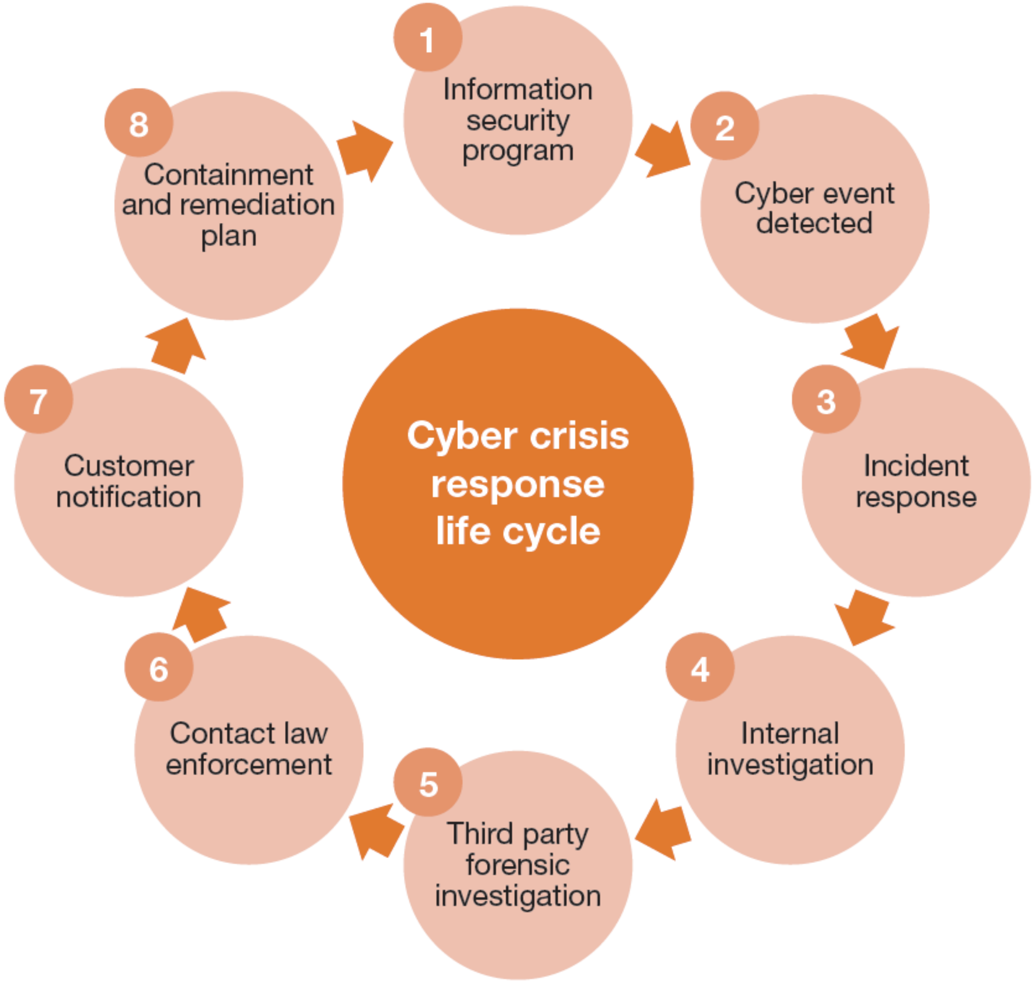
Outline

- Introduction
- Stages of Cyber Incident Response
- Challenges of Cyberspace
- Best practices

I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

BIRMINGHAM CITY University

Cyber Incident Response


Cyber crisis response life cycle
1
Information security program
2
Cyber event detected
3
Incident response
4
Internal investigation
5
Third party forensic investigation
6
Contact law enforcement
7
Customer notification
8
Containment and remediation plan

Preparation

- Threats/risks analysis
  - Operational, elevated, severe, strategic
- Strategies and resources
  - Guidelines for operations staff & first respondents, response & recovery teams, tools and trainings
- Management support
  - Boardroom awareness, allocation of resources
- Regular reviews and Exercises
  - Periodicity of reviews, gaps analysis, capability analysis

Detection

- Anomaly detection
  - Routine operations/processes are not running normally
  - Abnormal performance, crashes, etc.
- Complain received
  - Clients or operators signalled some problems

Detection is not easy for espionage attacks (Trojan horses) as they do not disrupt routine operations.

Efficient monitoring of processes is required to detect their presence.

Containment

- Containment strategy
  - Part of the incident response plan
  - Examples: full/partial shut-down, changing security controls, lock access to some services, moving to offline mode, ...
- Preserve the electronic evidence
  - To identify the action that triggered the incidence
  - Containment could be delayed to gather further information of attacker (Honeypot)

Containment through complete shutdown/offline has to be evaluated against the impact of service interruptions.

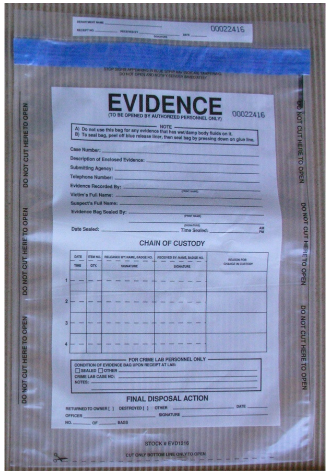
Analysis

- Generally third party specialised intervention
  - Evidence collection, examination, analysis and presentation

EnCase

FTK

nuix



sas

tableau SOFTWARE

Microsoft SQL Server

Relativity

Eradication

- Eliminating the cause of the incident
  - Removing malware, infected software/files, malicious accounts, ...
- Reset changes in the system parameters that were introduced by the attacker
  - SAM (Security Account Manager) database in Windows
  - .forward files in Linux/Unix
  - ...
- Quarantine
  - Enhanced monitoring of ports, logs, ...

Remediation

- Remediation of vulnerabilities
  - Installation of patches, more powerful antivirus, ...
- Restoration of the system
  - Full system restoration (from good media)
  - Restoration of data (from redundant drives, recent full backup, ...)
- Return to routine services
  - Normal logging and monitoring
  - Execution of regular business services

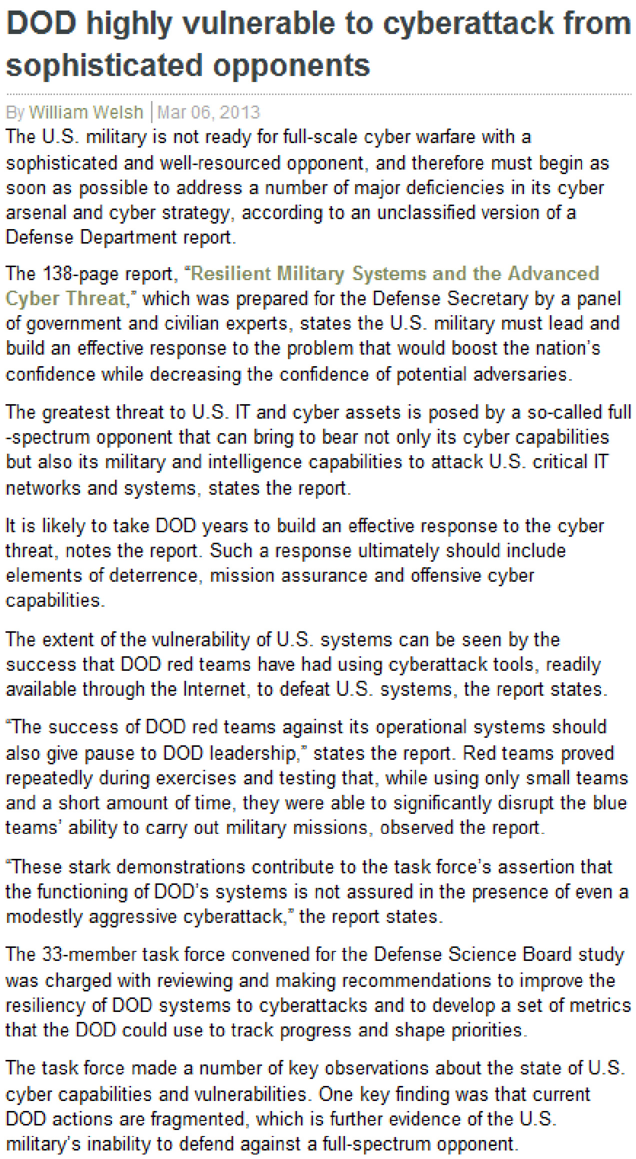
Follow-up

- Feedback
  - Preparation phase
  - Operations department
- Lessons learnt
  - Shortcomings and gaps
  - Communications and coordination
- Claims and settlements
  - Demarcation of responsibilities, litigation, ...

Dealing with sophisticated threats

- Better preparation
  - Timely and proactive installation of patches, fixes, new solution, ...
  - DRP (Disaster Recovery Planning) & BCP (Business Continuity Planning) should reflect the worst case scenarios for the cyber attacks.

- Deterrence
  - Stern administrative and legal actions against the collaborators/ perpetrators.



DOD highly vulnerable to cyberattack from sophisticated opponents

By William Welsh | Mar 06, 2013

The U.S. military is not ready for full-scale cyber warfare with a sophisticated and well-resourced opponent, and therefore must begin as soon as possible to address a number of major deficiencies in its cyber arsenal and cyber strategy, according to an unclassified version of a Defense Department report.

The 138-page report, "Resilient Military Systems and the Advanced Cyber Threat," which was prepared for the Defense Secretary by a panel of government and civilian experts, states the U.S. military must lead and build an effective response to the problem that would boost the nation's confidence while decreasing the confidence of potential adversaries.

The greatest threat to U.S. IT and cyber assets is posed by a so-called full -spectrum opponent that can bring to bear not only its cyber capabilities but also its military and intelligence capabilities to attack U.S. critical IT networks and systems, states the report.

It is likely to take DOD years to build an effective response to the cyber threat, notes the report. Such a response ultimately should include elements of deterrence, mission assurance and offensive cyber capabilities.

The extent of the vulnerability of U.S. systems can be seen by the success that DOD red teams have had using cyberattack tools, readily available through the Internet, to defeat U.S. systems, the report states.

"The success of DOD red teams against its operational systems should also give pause to DOD leadership," states the report. Red teams proved repeatedly during exercises and testing that, while using only small teams and a short amount of time, they were able to significantly disrupt the blue teams' ability to carry out military missions, observed the report.

"These stark demonstrations contribute to the task force's assertion that the functioning of DOD's systems is not assured in the presence of even a modestly aggressive cyberattack," the report states.

The 33-member task force convened for the Defense Science Board study was charged with reviewing and making recommendations to improve the resiliency of DOD systems to cyberattacks and to develop a set of metrics that the DOD could use to track progress and shape priorities.

The task force made a number of key observations about the state of U.S. cyber capabilities and vulnerabilities. One key finding was that current DOD actions are fragmented, which is further evidence of the U.S. military's inability to defend against a full-spectrum opponent.

Dealing with sheer volume of data

- Identify sensitive data
  - Structured and unstructured
  - Instances of data leakage
  - Intellectual property & trade secrets

- Advanced data analytics techniques and tools
  - Business intelligence
  - Data mining
  - Data visualisation
  - Big data

Focusing gigantic infrastructures

- Federated & flexible infrastructures
  - Elasticity
  - Abstraction/Virtualisation
  - Cross-border deployments

- Example: Cloud computing
  - Imaging of a Cloud require another Cloud
  - Analysis of a Cloud’s contents need power of an additional Cloud
  - Access details from terminal PCs

Sharing information & knowledge

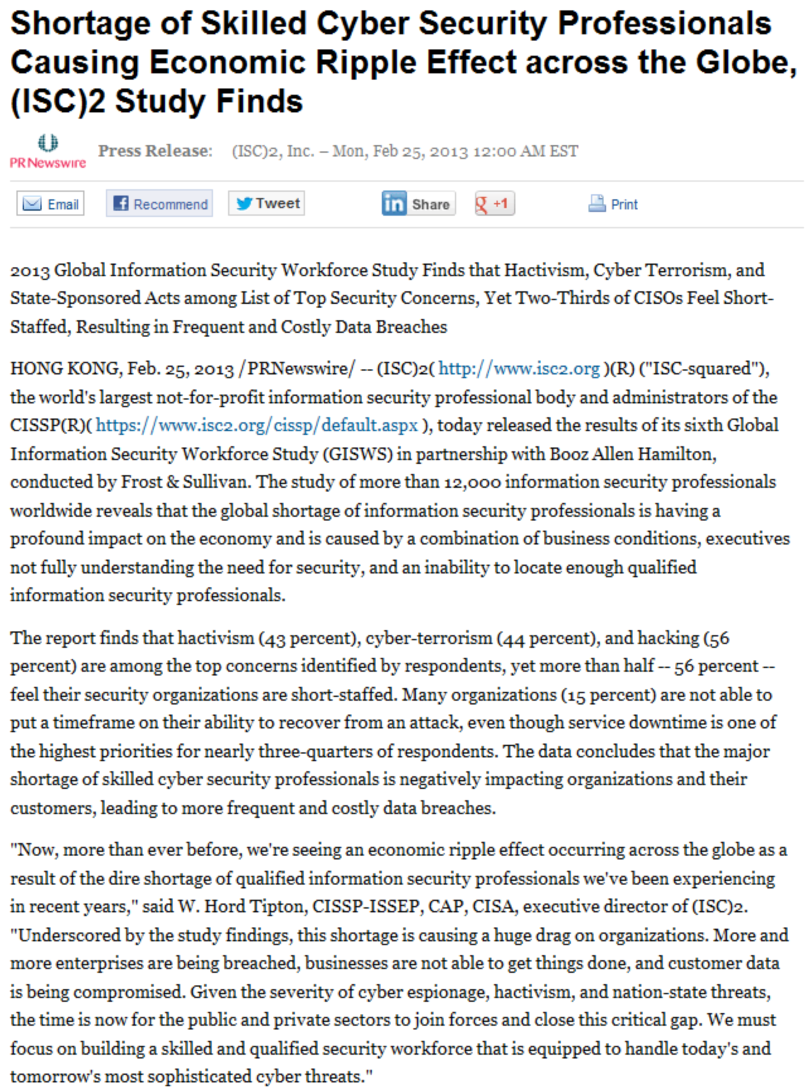
- Threat landscape is constantly evolving
  - Incident response planning requires knowledge of threat paradigm
  - Information related to vulnerabilities and their exploits helps improve contingency planning
- Sharing information and return of experience among the peers
  - Publication of exploits reports and lessons learnt
  - Sharing of detailed information through trusted parties – national CERTs
  - Without compromising corporate reputation!

Staff’s operational readiness

- Specialised training of the prospective Cyber fighters
  - Need to have such specialised training offerings
- Regular participation in refreshing courses & professional bodies
  - It is important for the cyber incident response team members to be ready to embrace the change
- Creation of Cyber reservists who can be called to reinforce cyber incident response teams
  - Could be third party specialists with framework agreement & NDA

Filling the skills gap

- Very specialised domain
- Scarcity of vocational/ educational programs
- Stakes are much higher than other fields
- Challenging environments requiring good level of knowledge



Shortage of Skilled Cyber Security Professionals Causing Economic Ripple Effect across the Globe, (ISC)2 Study Finds

Press Release: (ISC)2, Inc. – Mon, Feb 25, 2013 12:00 AM EST

2013 Global Information Security Workforce Study Finds that Hactivism, Cyber Terrorism, and State-Sponsored Acts among List of Top Security Concerns, Yet Two-Thirds of CISOs Feel Short-Staffed, Resulting in Frequent and Costly Data Breaches

HONG KONG, Feb. 25, 2013 /PRNewswire/ -- (ISC)2(http://www.isc2.org)(R) ("ISC-squared"), the world's largest not-for-profit information security professional body and administrators of the CISSP(R)(https://www.isc2.org/cissp/default.aspx), today released the results of its sixth Global Information Security Workforce Study (GISWS) in partnership with Booz Allen Hamilton, conducted by Frost & Sullivan. The study of more than 12,000 information security professionals worldwide reveals that the global shortage of information security professionals is having a profound impact on the economy and is caused by a combination of business conditions, executives not fully understanding the need for security, and an inability to locate enough qualified information security professionals.

The report finds that hactivism (43 percent), cyber-terrorism (44 percent), and hacking (56 percent) are among the top concerns identified by respondents, yet more than half -- 56 percent -- feel their security organizations are short-staffed. Many organizations (15 percent) are not able to put a timeframe on their ability to recover from an attack, even though service downtime is one of the highest priorities for nearly three-quarters of respondents. The data concludes that the major shortage of skilled cyber security professionals is negatively impacting organizations and their customers, leading to more frequent and costly data breaches.

"Now, more than ever before, we're seeing an economic ripple effect occurring across the globe as a result of the dire shortage of qualified information security professionals we've been experiencing in recent years," said W. Hord Tipton, CISSP-ISSEP, CAP, CISA, executive director of (ISC)2. "Underscored by the study findings, this shortage is causing a huge drag on organizations. More and more enterprises are being breached, businesses are not able to get things done, and customer data is being compromised. Given the severity of cyber espionage, hactivism, and nation-state threats, the time is now for the public and private sectors to join forces and close this critical gap. We must focus on building a skilled and qualified security workforce that is equipped to handle today's and tomorrow's most sophisticated cyber threats."

Cyber exercises

- The best way of testing an incident response plan
  - Coordination of different actors
  - Like integration testing of a product
  - Can be used as a deterrence tactic against potential attackers
- Helps observe the readiness of various stakeholders
  - Identifies gaps
  - Justifies remedies including resources allocation
- Expensive but more reliable evaluation mechanism
  - Like ‘Hot Sites” in DRP/BCP