Tarun kumar yadav
2014110
FCS Assignment 4

1) Look at the chief Security/Privacy leadership/executives' profiles of 3 US based Technology companies and 3 Indian based Technology companies like Flipkart, InMobi, etc. Look at the background each of these executives have. Make a comparison between the executives' profiles of the Indian Tech companies and the US Tech companies. Include a short note / bullet points about the security and privacy profiles(CISO / CPO).

USA Companies

Mike Howard (CISO at Microsoft)

- 13 Years at Microsoft - Chief Security Officer - CSO
- 22 Years at the Central Intelligence Agency
- 2 Years as a Police Officer - Oakland, California
- BS - Criminal Justice/Sociology - San Jose State University - 1980
- Martial Arts Expertise - Karate, Jiu-Jitsu, Aikido
- Married - No Children
- International Security Management Association (ISMA) Board of Directors, Past President.
- OSAC Advisory Council as of 2011 - Former Chair of the Fostering Innovation Council
- Security Industry Association Board of Directors as of 2011
- ASIS CSO Roundtable Advisory Board - 2012 - Currently President of CSO Roundtable Advisory Board
- Regularly asked to speak on Security and Leadership Issues
- Specialties: Experience in working with the U.S. Government and Corporate Security entities globally. Experience in working in foreign countries with extensive travel overseas.

Joe Sullivan (CSO at Uber)

Joe Sullivan is the Chief Security Officer(CSO) at Uber since April, 2015 till present and works in the San Francisco headquarters of Uber. He was the former CSO of the Facebook and worked there for 5 years from 2010 to 2015. He is responsible for all legal issues related to Regulatory, Privacy and Security. He was also the former Senior Director of the Trust and Safety Department of eBay Incorporation. He did his B.A. degree in Political Science from Providence College from 1986-90. After pursuing B.A. degree, he also did J.D. in Law from the University of Miami School of Law from 1990-93.

John McClurg (CSO at Dell)

John E. McClurg serves as Vice President and Ambassador-At-Large at Cylance. Is responsible for building Security and Trust programs, operational excellence efforts. Engages the industry around the globe on the risk challenges today and how Cylance uniquely mitigates them with the application of machine learning with CylancePROTECT®.

Champions a move from a historically reactive security posture to one focused on proactively predicting and mitigating future risks.Before Cylance, McClurg served as Dell's CSO, where his responsibilities included the strategic focus and tactical operations of Dell’s internal global security service. Was also charged with the advocacy of business resilience and security prowess, the seamless integration of Dell’s security offerings, and with improving the effectiveness and efficiency of security initiatives. Before Dell, McClurg served as the VP of Global Security at Honeywell International; Lucent/Bell Laboratories; and in the US Intel Community, as a twice-decorated member of the FBI, where he held an assignment with the US Dept of Energy (DOE) as a Branch Chief charged with establishing a Cyber-Counterintelligence program within the DOE’s newly created Office of Counterintelligence. Prior to that, McClurg served as a FBI Supervisory Special Agent, assisting in the establishment of the FBI’s new Computer Investigations and Infrastructure Threat Assessment Center or what is today known as the National Infrastructure Protection Center within the Dept of Homeland Security. McClurg also served, on assignment as a Deputy Branch Chief with the CIA, helping to establish the new Counterespionage Group and was responsible for the management of complex counterespionage investigations. He also served as a Special Agent for the FBI in the Los Angeles Field Office where he implemented plans to protect critical US technologies targeted for unlawful acquisition by foreign powers and served on one of the nation’s first Joint Terrorism Task Forces.

INDIAN Companies

Sameer Ratolikar (CISO at HDFC)

Presently working as CISO -Chief Information Security Officer at HDFC Bank, Mumbai , India.

Previously Worked as CISO In Axis Bank and as CTO and CISO at Bank Of India .

-Worked as Principal Systems Analyst(Security & networks) in Ministry of IT on deputation to Govt. of Gujarat-
-Believes in thought leadership and developing strategies to achieve goals
-Active Information Security, PRIVACY and Cyber Crime speaker in various national and international conferences
-Pioneer in Indian banking industry for achieving ISO 27001 , PCI-DSS and BS25999 certification for the Bank
Written a book " Information Security-Demystified" for bank's users and employees .
- Firm believer of role of CISO as a risk manager

-Pioneer in the industry to establish ZACHMAN framework and SABSA based Information security architecture
-Firm beliver that success of Info-security lies in integration of People-Processes and Technology facilitated by Information Security strategies, Governance and a robust security architecture .
-On the panel of Regulators and IBA on developing "Security Standard for indian banks"
- Implemented huge security projects like 2FA, Data leakage prevention, Identity & Access management, GRC, SOC, PCI-DSS , ISO 27001 , Business Continuity across major BUs of the Bank.
-worked on all domains of Information security .viz.. Enterprise , infrastructure, application and finally data protection/ Privacy
-Sound grip over relevant legal and regulatory requirements, such as SOX, HIPPA, RBI guidelines, MAS guidelines, FFIEC guidelines, UK Data Protection act
-Member of various national and International Data Protection and security forums
- Very good knowledge of various security tools and technologies

Subrahmanya Gupta Boda (CISO GMR infrastructure limited)

Implementing reasonable information security practices across GMR Group companies.

Experienced with Application Development & Support, IT Service Delivery, IT Infrastructure Management and Information Security in a large automotive MNC in Captive and Enterprise environment.

Specialties: Information Security Management Systems (ISO 27001)
Indian IT Act (Amendment) 2010
IT Infrastructure Continuity Management (BS 25999)
Information Technology Infrastructure Library (ITIL) V2/V3
Capability Maturity Model Integrated
Sarbanes-Oxley Act for IT - IT General Controls (COBIT)
Personal Software Process (PSP)
Software Development Life Cycle (SDLC)
Program Office / Project Management Office (PMBoK)
Business Analysis Body of Knowledge (BABoK)
Software Engineering Body of Knowledge (SWBOK) of IEEE

Anuj Tewari (CISO at HCL Technologies)

Currently hold the following key credentials

- CISSP ® - Certified Information Systems Security Professional
- CISA ® - Certified Information Systems Auditor
- CISM ® - Certified Information Security Manager
- CIPT ® - Certified Information Privacy Technologist
- CCSK ® - Certificate of Cloud Security Knowledge
- CEH ® - Certified Ethical Hacker
- ISO 27001LA, BS25999 LA, ITIL v3, ITSM, MCSE - Security Track, CCNA

- Ensure Business Units set budgets in line with company plans. Review the progress of these budgets to ensure that they are met
- Plan and ensure development of competencies so that continued revenue streams in future are assured
- Maintain executive level connect with customers so that relationships are strengthened and accounts continue to grow
- Ensure quality delivery on time within budget, and managing systems and processes are in line with the scale of the operations
- Large Scale, Global Service Operations
- Strategic Planning & Re-Positioning
- New Product/Service Design & Launch, M&A Integration
-Active Information Security, Privacy and Cyber warfare speaker in various national and international conferences
- Firm believer of role of CISO as a risk manager
- Worked on all domains of Information security Enterprise, infrastructure, application and data protection and Privacy
- Member of various national and International Data Protection and security forums

Differences:-

Foreign companies:-

1) CPOs are more common in US companies but most big companies have

CSOs like Microsoft.

2) US CPOs/CSOs usually have a law degrees.

3) US CSOs/CPO’s usually climbs little by little to reach that position.

4) They generally sticks to their jobs.

Indian companies:-

1) CISOs are more common in Indian companies and CPOs are difficult to find

in some of the big companies also.

2) CISOs generally have technical degrees.

3) CISOs are generally post-graduates in business/finance.

4) They pile up degrees and frequently change their jobs.

Question2) Last week, as was noted on Backpack as well, there were a wave of massive DDOS attacks in the USA which caused major websites such as Twitter and Spotify to go down.[10+10+5]
a.Investigate and critique the cause of these attacks : how were they deployed?
b.Suggest technical mitigations
c.Suggest Judicial changes that could prevent such an attack in future
Please restrict the context to these recent attack only

a) Causes of the attack and their deployment:- This websites go down because the attackers didn't target specific sites but they attacked massively on DYN's DNS infrastructure. It is a system that resolves the web addresses into the IP addresses needed by browsers to connect with right
servers and deliver the requested content. DYN is a company that provides core Internet services for Twitter, SoundCloud, Spotify, Reddit and a host of other sites i.e. taking down DYN means taking down all these sites as well. That's why impact of this attack was quite large. A botnet (a network of computer that are infected with a special malware) was used to bombard the DYN's DNS infrastructure until the load become too much to handle for the server and became unresponsive. The botnet was a special botnet. It is a Miria botnet i.e. it is made of Internet of Things (IOT) devices like DVRs etc. Large number of devices connected to the need made the attack much more effective than a normal botnet. Internet of Things insecurity problem and lack of an effective combative strategy were the loopholes that were exploited by the attackers.

b) Technical Mitigations:-

By countering these attacks by absorbing them with a global network of scrubbing centres that scale, on demand, to counter multi-gigabyte DDoS attacks.
by blocking bad traffic before it even reaches the site, leveraging visitor identification technology that differentiates between legitimate
website visitors (humans, search engines etc.) and automated or malicious clients.
by monitoring visitor behavior, blocking known bad bots, and challenging suspicious or unrecognized entities with JS test, Cookie challenge, and even CAPTCHAs.

Know your customers and lock out unexpected transactions.
Include performance and architecture to deploy upstream to protect all points of vulnerability.
Identify and blocks individual spoofed packets to protect legitimate business transactions.
Implement mechanisms such as source-based remotely-triggered blackholes(S/RTBH), flowspec.
Scan for both vulnerable and compromised IOT devices on their networks and the networks of the customers and then isolate those devices, notify their owners of the problem and ask them to take action.

Judicial changes
One of the most salient points from the attack on Dyn is that it highlights the need for stronger standards and protocols for security in the IoT industry.We need to begin to hold IoT device manufacturers to the same standards of security that we hold operating system and application developers to in the tech world. If IoT vendors are allowed to produce products with known vulnerabilities, we will likely see more attacks like this one

3.Code a Keylogger. You can follow online tutorials but please do not plagiarize code from other students or from online. [10 marks]
File attached . Run keylogger.py

4. Install Burp Suite. Follow the instructions given here to set it up on your laptop and install a certificate on your mobile. Filter Facebook related traffic from your phone and see if you can find any security/privacy related vulnerabilities. [15 marks]

a) We can get the id of the person from which we can uniquely identify the person. This may lead to breach in privacy, as we can open the profile of the person using that referrer id.

b) Whenever we search something on facebook (using search option), the unique id of that person get caught in the burp. This is also a breach in privacy. As we can easily find what a person is doing (searching) on facebook.

c) Proxy server get(catches) all the data of the post, whatever user posts. And even if user deletes the post, we can have a copy the data.

5. Differentiate between the Biba Model and the Bell-LaPadula Model. Apply both models on the following scenario: [10+5+5]
a.IIITD Accounts Department has the following 4 roles: Administrator, Accounts

Keeper, Manager and Clerk in their order of hierarchy. Not all of them have access to the same amount of information.
b.Define object classes based on your requirements.After applying both models
which do you think is the better?
c.Justify your answer

Bell-LaPadula Model

1. Very High Level Transactions(Top Secret)

READ PERMISSION : Administrator
WRITE PERMISSION : All Subjects

2. High Level Transactions(Secret)

READ PERMISSION : Administrator and Accounts Keeper
WRITE PERMISSION : Accounts Keeper, Manager and Clerk

3. Medium Level Transactions(Confidential)

READ PERMISSION : Administrator, Accounts Keeper and Manager
WRITE PERMISSION : Manager and Clerk

4. Low Level Transactions(Unclassified)

READ PERMISSION : All Subjects
WRITE PERMISSION : Clerk

Biba Model

1. Very High Level Transactions(Top Secret)

READ PERMISSION : All Subjects
WRITE PERMISSION : Administrator

2. High Level Transactions(Secret)

READ PERMISSION : Accounts Keeper, Manager and Clerk
WRITE PERMISSION : Administrator and Accounts Keeper

3. Medium Level Transactions(Confidential)

READ PERMISSION : Manager and Clerk
WRITE PERMISSION : Administrator, Accounts Keeper and Manager

4. Low Level Transactions(Unclassified)

READ PERMISSION : Clerk
WRITE PERMISSION : All Subjects

Conclusion:

I think Bell Lapadula method should be applied. So that information about Top secret transactions or transactions at top level should not be leaked to the officials lower in the hierarchy like the Clerks unless he/she wrote it himself/herself. Only the administrator must have this facility.Allowing the persons lower in hierarchical, could lead to security breach and misuse of critical information.