21st ACG Cross Training Seminar

Thursday, February 28, 2019

Cyber Security

Central Depository Company of Pakistan Limited (CDCPL)

Agenda

- Introduction
- Cyber Space
- Cyber Crime
- Brief History of Cyber Crime
- Main Targets of Cyber Crime
- Cyber Security

Agenda

- CDCPL Vision/Mission
- Three Pillars @ CDCPL
- Cyber Security @ CDCPL perspective
- Conclusion

Cyber Space

- Cyberspace refers to the virtual computer world. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyber Crime

- Cybercrime, or computer-oriented crime, is the crime that involves a computer and a network.

Types of Cyber Crime

1. Social Engineering
2. Denial of Service a.k.a (DOS)
3. Virus Dissemination
4. Malicious Code
5. Forgery
6. Malware
7. Phishing
8. Spam
9. Spoofing
10. Ransomware

Brief History of Cyber Crime

- First Cyber Crime (1970)

  One of the first computer-related crimes ever recorded was committed by an employee of the Park Avenue branch of New York's Union Dime Savings Bank, who used a computer to syphon over1.5m from hundreds of customer bank account.

- Personal Computer Evolution (1980)

  First known PC virus called 'Brain' was written by two brothers .

Brief History of Cyber Crime

- Ransomware (1989)

The first known ransom ware was 'AIDS' Trojan, also known as 'PC cyborg'

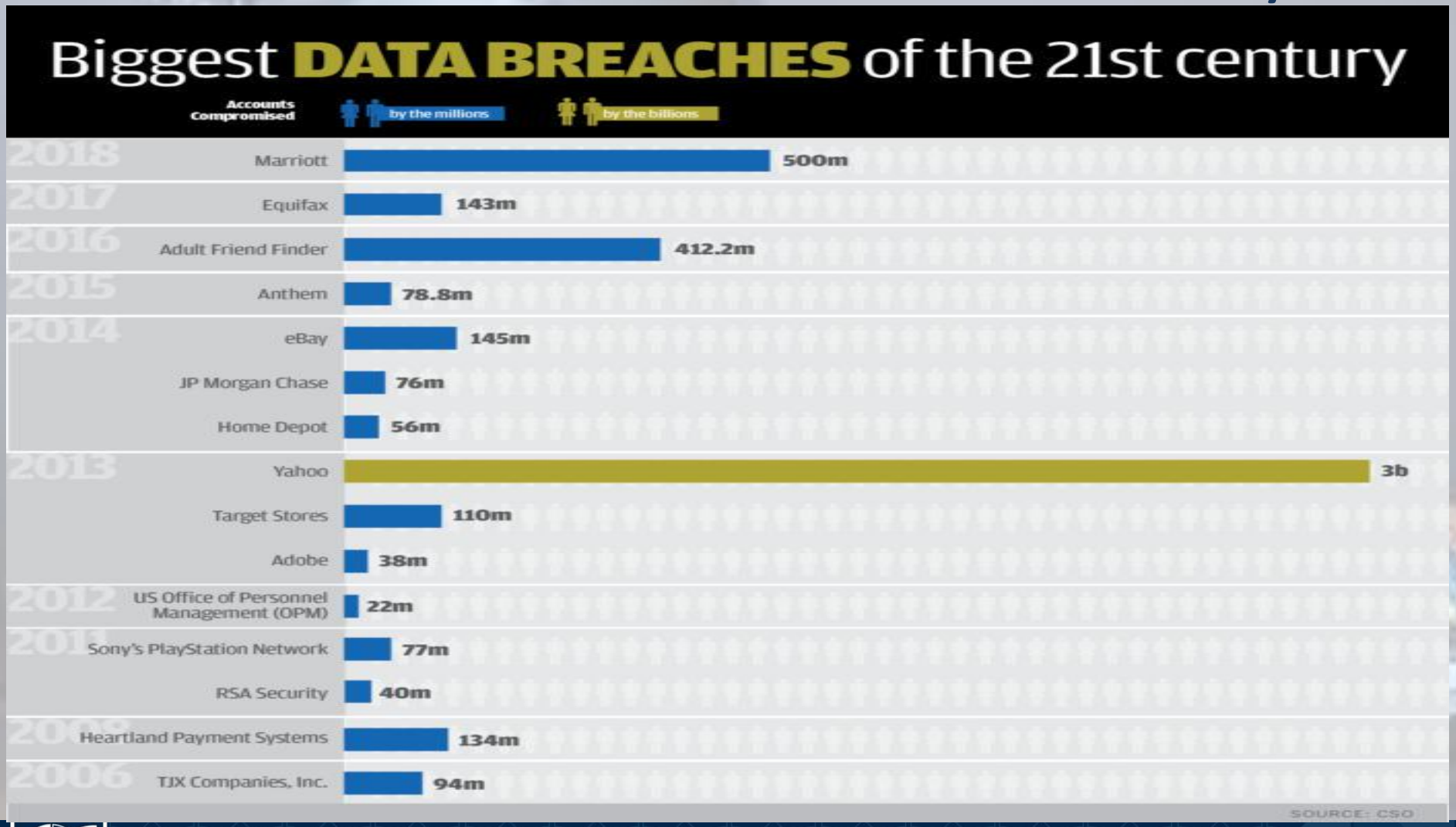
- Birth of Internet (1990)

The advent of internet has not only created ripples in digital revolution but it also brings the plethora of security risks along with it. New threats such as 'DDOS', Online fraud etc enters the cyberspace after in this era.

Main Targets of Cyber Crime

- Individual
- Corporates/Businesses
- Nation/States

Notable Breaches in 21st Century



Cyber Security

- Mechanism to defend the cyber space from cyber crime. Confidentiality, Integrity and Processes is the doctrine that govern cyber security.

CIA : Three Pillars of Cyber Security

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Three Pillars of Cyber Security

CIA @ People

Every employee needs to be aware of their role in preventing and reducing cyber threats, and specialized technical cyber security staff need to stay fully up to date with the latest skills and qualifications to mitigate and respond to cyber attacks.

Three Pillars of Cyber Security

CIA @ Processes

Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information. Cyber threats change quickly, so processes need to be continually reviewed to be able to adapt alongside them.

Three Pillars of Cyber Security

CIA @ Technology

By identifying the cyber risks that your organization faces you can then start to look at technologies you'll need to do this. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk.

CDCPL Vision / Mission

- Provide **SECURE**, reliable and innovative solutions that systematically reduce risk, enable transparency and bring efficiencies to Capital & Financial markets.

- Stimulating business growth and maximizing benefits for all stakeholders.

People @ CDCPL

- Humans are the weakest links. Modern day attacks are mostly driven by social engineering. So it is imperative to educate and train the users.
- CDCPL conducts regular security awareness trainings of all staffs including clients, third party contractors and vendors to ensure that users using CDCPL system(s) are well aware of the threats CDCPL is facing.
- To make awareness more effective, CDCPL has an eLearning portal to ensure all the staff can easily login to eLearning portal to get the security related content anytime.

Processes @ CDCPL

- CDCPL is ISO/IEC 27001:2013 certified for Information Security Management
- CDCPL is Pakistan's first company to receive ISO 22301 certification for its Business Continuity Management Program.
- CDCPL is also certified with ISAE 3402.

Technology @ CDCPL

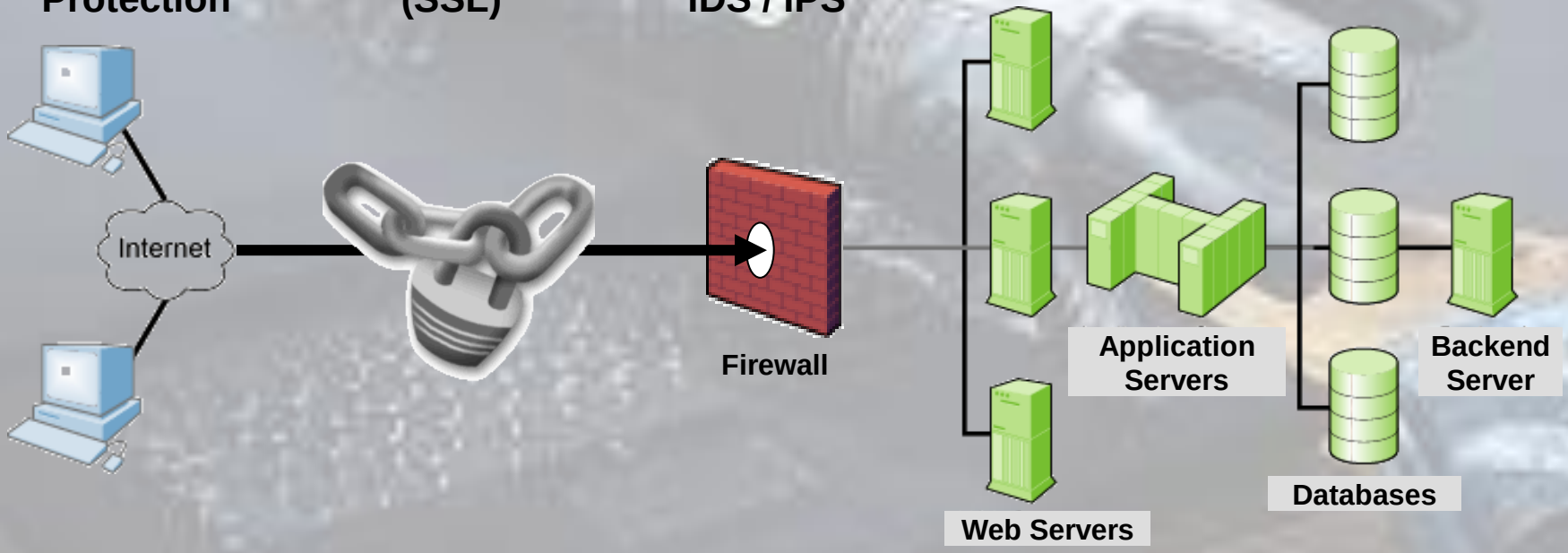
- CDCPL conducts vulnerability scans of all its production on a daily and weekly basis.
- All internet exposed web applications are protected with application firewalls.
- CDCPL has deployed state-of-the-art SIEM solution, IPS, Firewalls and Anti-virus solutions.
- CDCPL also conducts third party penetration testing by engaging expert firms.

Application Security

- One of the several levels of security that encompasses measures taken to improve the security of an application by finding, fixing and preventing security vulnerabilities.

Info Security Landscape

Desktop	Transport	Network	Web Applications
Antivirus Protection	Encryption (SSL)	Firewalls / IDS / IPS	



Application Security

- What's Happening?

"The security industry is overly-focused on testing and scanning for known vulnerabilities in software after it's been released, and under-focused on poor software development practices that lead to vulnerable applications that hackers can exploit".

(Frank Zinghini, CEO of Applied Visions, Inc.)

Application Security Challenges/Threats (OWASP Top 10)

Application Threat	Negative Impact	Example Impact
Cross Site scripting	Identity Theft, Sensitive Information Leakage, …	Hackers can impersonate legitimate users, and control their accounts.
Injection Flaws	Attacker can manipulate queries to the DB / LDAP / Other system	Hackers can access backend database information, alter it or steal it.
Malicious File Execution	Execute shell commands on server, up to full control	Site modified to transfer all interactions to the hacker.
Insecure Direct Object Reference	Attacker can access sensitive files and resources	Web application returns contents of sensitive file (instead of harmless one)
Cross-Site Request Forgery	Attacker can invoke "blind" actions on web applications, impersonating as a trusted user	Blind requests to bank account transfer money to hacker
Information Leakage and Improper Error Handling	Attackers can gain detailed system information	Malicious system reconnaissance may assist in developing further attacks
Broken Authentication & Session Management	Session tokens not guarded or invalidated properly	Hacker can "force" session token on victim; session tokens can be stolen after logout
Insecure Cryptographic Storage	Weak encryption techniques may lead to broken encryption	Confidential information (SSN, Credit Cards) can be decrypted by malicious users
Insecure Communications	Sensitive info sent unencrypted over insecure channel	Unencrypted credentials "sniffed" and used by hacker to impersonate user
Failure to Restrict URL Access	Hacker can access unauthorized resources	Hacker can forcefully browse and access a page past the login page

Best Practices (OWASP Top 10)

Application Threat	Best Practice
Cross Site Scripting	• Escape all user input • Do not accept and reflect unsolicited input
Injection Flaws	• Use Prepared Statement • Validate Inputs
Malicious File Execution	• Architect and Design • Add firewall to restrict external website connection
Insecure Direct Object Reference	• Validate data on server side • Do not expose internals to the user.
Cross-Site Request Forgery	• Add secondary authentication mechanism • Use “POST” instead of “GET” as form action
Information Leakage and Improper Error Handling	• Apply timely patch • Avoid directory browsing
Broken Authentication and Session Management	• Use built in session management • Use secure and random generated session keys • Use reasonable session timeouts
Insecure Cryptographic Storage	• Use latest and strong encryption methods. • Store passwords based on strong algorithms i.e. (SHA-256,AES,RSA)
Insecure Communication	• Use SSL
Failure to Restrict URL Access	• Implement proper authentication and authorization

Application Security

- What's Required?

  "A far better model (for software development) would be if you were teaching your developers how to write secure code, were including security architects in the development process from day one of the project, and investing in tools for secure development. Then you have many fewer flaws at the end of the process.". (James Kaplan, a partner at McKinsey & Co.)

Conclusion

- Chain is as strong as its weakest link

- No 'Silver bullet' solution

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and its money wasted; none of these measures address the weakest link in the security chain."

Kevin Mitnick, One of The World's Most Famous Hackers. (Source: The Economist)