Introduction to Cybersecurity

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

Introduction of Instructor & Course

Scope & Need of Cybersecurity

Scope

Personal Security

Business and Corporate Security

Financial Security

Healthcare Security

Critical Infrastructure Security

Government and Public Sector Security

Education Security

Internet of Things (IoT) Security

Scope & Need of Cybersecurity

Need

Safeguarding Personal Information

Prevention of Identity Theft

Business Continuity

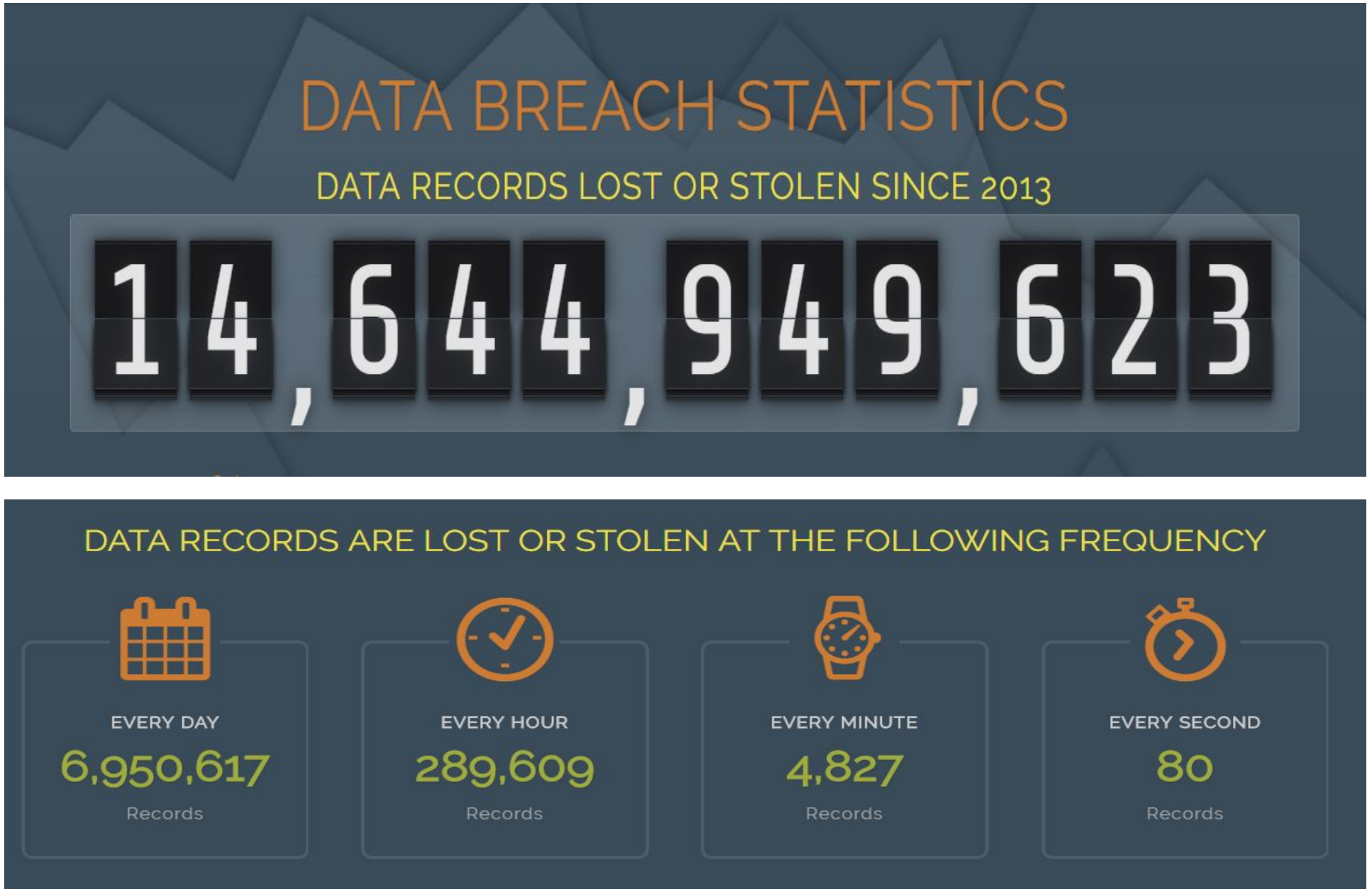
Protection of Intellectual Property

Financial Security

Preservation of National Security

Attack on Iran's Nuclear Facility

1. Stuxnet is a computer worm discovered in June 2010
2. It initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment
3. Took the control of functioning of a nuclear power plant.
4. After the damage is done, Stuxnet is designed to self-destruct so it is very hard to trace.


DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
14,644,949,623
DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY
EVERY DAY
6,950,617
Records
EVERY HOUR
289,609
Records
EVERY MINUTE
4,827
Records
EVERY SECOND
80
Records

What do we Protect?

Unauthorised Modification

Unauthorised Deletion

Unauthorised Access

Sources of Threats

Cyber threats can come from a wide variety of sources, some notable examples include:

1. National governments.
2. Terrorists.
3. Rogue employees.
4. Hackers.
5. Business competitors.
6. Organization insiders.

Causes of Compromised Security

Job Roles in Cybersecurity

Security Analyst

Security Engineer

Penetration Tester (Ethical Hacker)

Security Consultant

Security Architect

Security Software Developer

Incident Responder

Security Auditor

Security Researcher

Forensic Analyst

Security Awareness and Training Specialist

Practice:

https://tryhackme.com/room/securityawarenessintro

Students are advised to create a THM account from their professional account.

CIA Traid

Related article: https://www.fortinet.com/resources/cyberglossary/cia-triad

The CIA Triad refers to three core principles that form the foundation of information security. The acronym CIA stands for Confidentiality, Integrity, and Availability. The CIA Triad is like a three-part guide to keeping information safe.

Confidentiality: Keep information a secret. Only the people who should see it are allowed to see it.

Integrity: Make sure information is correct and hasn't been changed by mistake or on purpose.

Availability: Ensure that information is always accessible when it's needed.

RED TEAM

OFFENSIVE ATTACK TEAM

Tasks include:

- Ethical hacking
- Penentration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulernability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM

Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics

Benefits of Linkedin

1. Networking Opportunities
2. Job Search and Recruitment
3. Personal Branding
4. Professional Visibility
5. Knowledge Sharing and Thought Leadership
6. Recommendations and Endorsements
7. Learning and Professional Development
8. Company Research
9. Showcasing Portfolio and Projects
10. Global Reach
11. Continuous Professional Updates

Resources to Create a Professional Linkedin Profile:

1. How to Use Linkedin – Hisham Server
2. 5 Must-Know Linkedin Profile Tips
3. How to Make a Great Linkedin Profile

THANK YOU

Recommended Video

Introduction to Cybersecurity