CYBER SECURITY STRATEGIES

http://www.tutorialspoint.com/information_security_cyber_law/cyber_security_strategies.htm
Copyright © tutorialspoint.com

To design and implement a secure cyberspace, some stringent strategies have been put in place. This chapter explains the major strategies employed to ensure cybersecurity, which include the following −

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework
- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure

Strategy 1 − Creating a Secure Cyber Ecosystem

The cyber ecosystem involves a wide range of varied entities like devices *communicationtechnologiesandcomputers*, individuals, governments, private organizations, etc., which interact with each other for numerous reasons.

This strategy explores the idea of having a strong and robust cyber-ecosystem where the cyber-devices can work with each other in the future to prevent cyber-attacks, reduce their effectiveness, or find solutions to recover from a cyber-attack.

Such a cyber-ecosystem would have the ability built into its cyber devices to permit secured ways of action to be organized within and among groups of devices. This cyber-ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.

A strong cyber-ecosystem has three symbiotic structures − **Automation, Interoperability,** and **Authentication**.

- **Automation** − It eases the implementation of advanced security measures, enhances the swiftness, and optimizes the decision-making processes.
- **Interoperability** − It toughens the collaborative actions, improves awareness, and accelerates the learning procedure. There are three types of interoperability −
    - Semantic *i. e. , sharedlexiconbasedoncommonunderstanding*
    - Technical
    - Policy − Important in assimilating different contributors into an inclusive cyber-defense structure.
- **Authentication** − It improves the identification and verification technologies that work in order to provide −
    - Security
    - Affordability
    - Ease of use and administration
    - Scalability
    - Interoperability

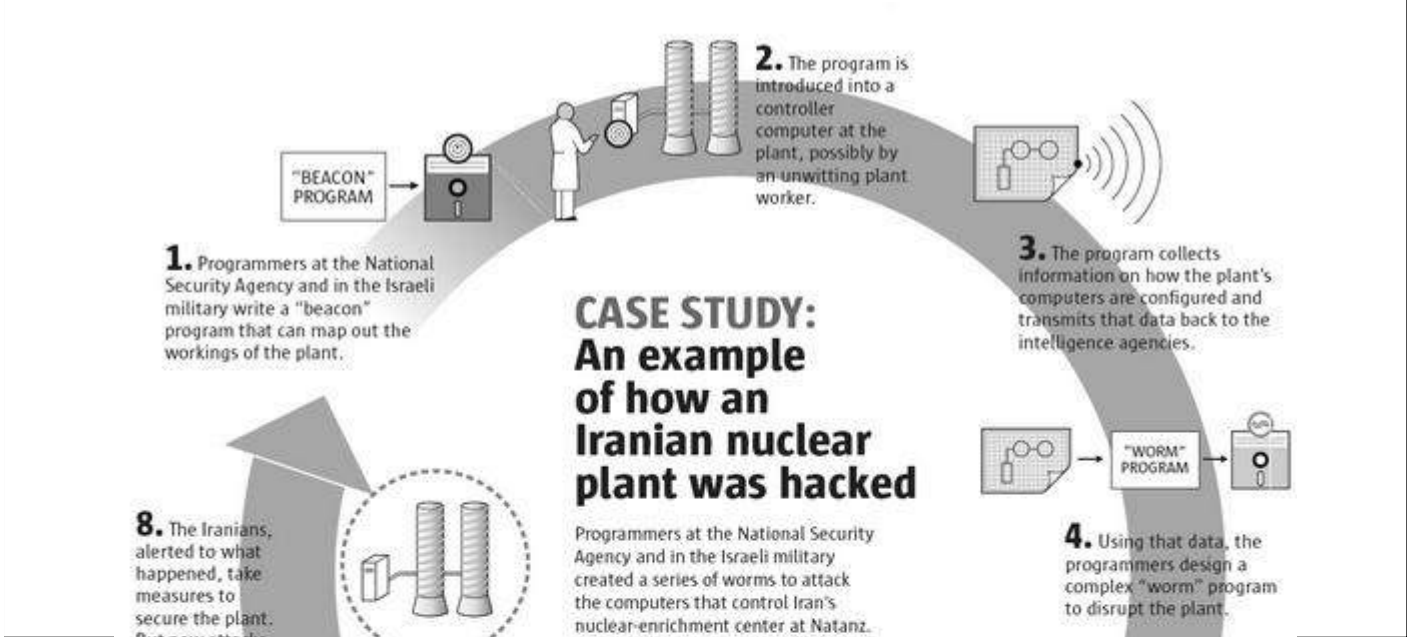
Comparison of Attacks

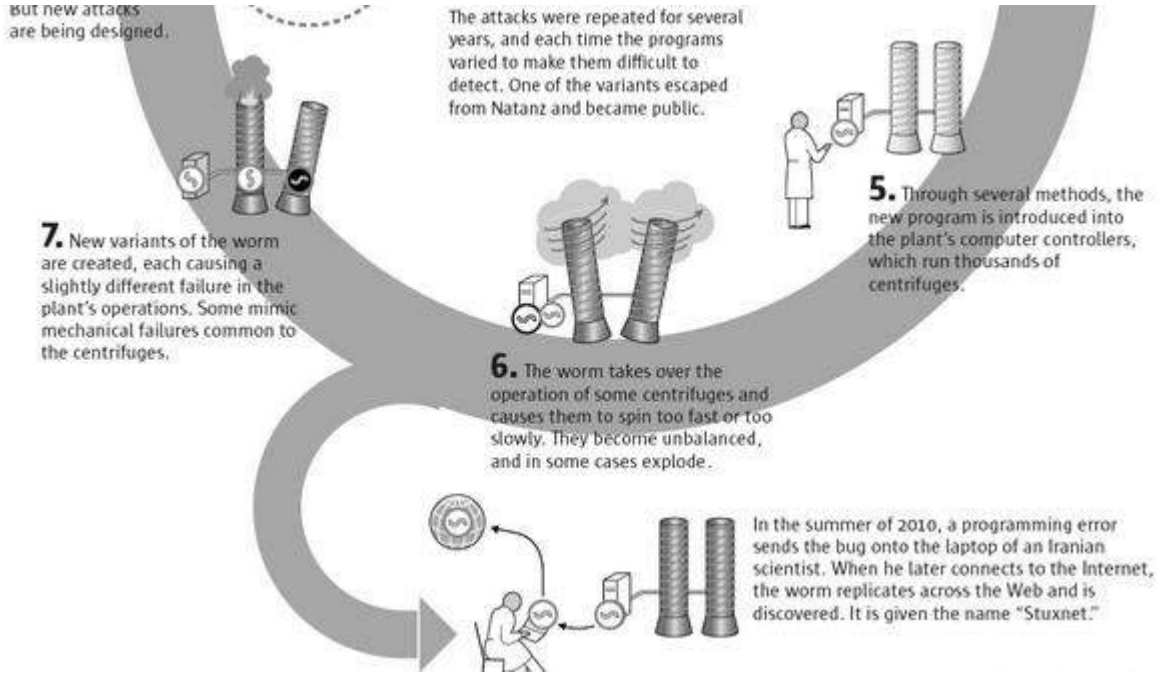
The following table shows the *Comparison of Attack Categories against Desired Cyber Ecosystem Capabilities* −

	Categories of Cyber Attack							
Desired Cyber Ecosystem Capabilities	**Attrition**	**Malware**	**Hacking**	**Social Tactics**	**Improper Usage (Insider)**	**Physical Action; Loss or Theft**	**Multiple Component**	**Other**
Automation	x	x	x	x	x	x	x	x
Authentication	x	x	x	x		x	x	x
Interoperability	x	x	x	x			x	
Automated Defense Identification, Selection, and Assessment	x	x	x	x	x	x	x	x
Build Security In	x	x	x	x		x	x	x
Business Rules-Based Behavior Monitoring	x	x	x	x	x	x	x	x
General Awareness and Education	x	x	x	x	x	x	x	x
Moving Target	x	x	x	x			x	x
Privacy	x	x	x	x	x	x	x	x
Risk-Based Data Management	x	x	x	x	x	x	x	x
Situational Awareness	x	x	x	x	x	x	x	x
Tailored Trustworthy Spaces	x	x	x	x			x	x

Case Study

The following diagram was prepared by ***Guilbert Gates for The New York Times,*** which shows how an Iranian plant was hacked through the internet.





Explanation − A program was designed to automatically run the Iranian nuclear plant. Unfortunately, a worker who was unaware of the threats introduced the program into the controller. The program collected all the data related to the plant and sent the information to the intelligence agencies who then developed and inserted a worm into the plant. Using the worm, the plant was controlled by miscreants which led to the generation of more worms and as a result, the plant failed completely.

Types of Attacks

The following table describes the attack categories −

Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following − • distributed denial of service attacks • impair or deny access to a service or application • resource depletion attacks
Malware	Any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.
Hacking	An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include − • data-leakage attacks • injection attacks and abuse of functionality • spoofing • time-state attacks • buffer and data structure attacks • resource manipulation • stolen credentials usage

	• backdoors • dictionary attacks on passwords • exploitation of authentication
Social Tactics	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes − • pre-texting *forgedsurveys* • inciting phishing • retrieving of information through conversation
Improper Usage *InsiderThreat*	Misuse of rights to data and controls by an individual in an organization that would violate the organization's policies. It includes − • installation of unauthorized software • removal of sensitive data
Physical Action/Loss or Theft of Equipment	Human-Driven attacks such as − • stolen identity tokens and credit cards • fiddling with or replacing card readers and point of sale terminals • interfering with sensors • theft of a computing device used by the organization, such as a laptop
Multiple Component	Single attach techniques which contains several advanced attack techniques and components.
Other	Attacks such as − • supply chain attacks • network investigation

Strategy 2 − Creating an Assurance Framework

The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.

To cater to the national security requirements, a national framework known as the **Cybersecurity Assurance Framework** was developed. It accommodates critical infrastructure organizations and the governments through "Enabling and Endorsing" actions.

Enabling actions are performed by government entities that are autonomous bodies free from commercial interests. The publication of "National Security Policy Compliance Requirements" and IT security guidelines and documents to enable IT security implementation and compliance are done by these authorities.

Endorsing actions are involved in profitable services after meeting the obligatory qualification standards and they include the following −

- ISO 27001/BS 7799 ISMS certification, IS system audits etc., which are essentially the compliance certifications.
- 'Common Criteria' standard ISO 15408 and Crypto module verification standards, which are the IT Security product evaluation and certification.
- Services to assist consumers in implementation of IT security such as IT security manpower training.

Trusted Company Certification

Indian IT/ITES/BPOs need to comply with the international standards and best practices on security and privacy with the development of the outsourcing market. ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., are some of the certifications.

Existing models such as SEI CMM levels are exclusively meant for software development processes and do not address security issues. Therefore, several efforts are made to create a model based on self-certification concept and on the lines of Software Capability Maturity Model $SW-CMM$ of CMU, USA.

The structure that has been produced through such association between industry and government, comprises of the following −

- standards
- guidelines
- practices

These parameters help the owners and operators of critical infrastructure to manage cybersecurity-related risks.

Strategy 3 − Encouraging Open Standards

Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to −

- Enhance the efficiency of key processes,
- Enable systems incorporations,
- Provide a medium for users to measure new products or services,
- Organize the approach to arrange new technologies or business models,
- Interpret complex environments, and
- Endorse economic growth.

Standards such as ISO 27001[3] encourage the implementation of a standard organization structure, where customers can understand processes, and reduce the costs of auditing.

Strategy 4 − Strengthening the Regulatory Framework

The objective of this strategy is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure Protection Centre $NCIIPC$. The Computer Emergency Response Team $CERT-In$ has been designated to act as a nodal agency for crisis management.

Some highlights of this strategy are as follows −

- Promotion of research and development in cybersecurity.
- Developing human resource through education and training programs.
- Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer $CISO$ who will be responsible for cybersecurity initiatives.
- Indian Armed Forces are in the process of establishing a cyber-command as a part of

strengthening the cybersecurity of defense network and installations.

- Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

Strategy 5 − Creating Mechanisms for IT Security

Some basic mechanisms that are in place for ensuring IT security are − link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption. These methods differ in their internal application features and also in the attributes of the security they provide. Let us discuss them in brief.

Link-Oriented Measures

It delivers security while transferring data between two nodes, irrespective of the eventual source and destination of the data.

End-to-End Measures

It is a medium for transporting Protocol Data Units *PDUs* in a protected manner from source to destination in such a way that disruption of any of their communication links does not violate security.

Association-Oriented Measures

Association-oriented measures are a modified set of end-to-end measures that protect every association individually.

Data Encryption

It defines some general features of conventional ciphers and the recently developed class of public-key ciphers. It encodes information in a way that only the authorized personnel can decrypt them.

Strategy 6 − Securing E-Governance Services

Electronic governance $e-governance$ is the most treasured instrument with the government to provide public services in an accountable manner. Unfortunately, in the current scenario, there is no devoted legal structure for e-governance in India.

Similarly, there is no law for obligatory e-delivery of public services in India. And nothing is more hazardous and troublesome than executing e-governance projects without sufficient cybersecurity. Hence, securing the e-governance services has become a crucial task, especially when the nation is making daily transactions through cards.

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 1st October, 2013. It has put the responsibility of ensuring secured card transactions upon banks rather than on customers.

"E-government" or electronic government refers to the use of Information and Communication Technologies *ICTs* by government bodies for the following −

- Efficient delivery of public services
- Refining internal efficiency
- Easy information exchange among citizens, organizations, and government bodies
- Re-structuring of administrative processes.

Strategy 7 − Protecting Critical Information Infrastructure

Critical information infrastructure is the backbone of a country’s national and economic security. It includes power plants, highways, bridges, chemical plants, networks, as well as the buildings where millions of people work every day. These can be secured with stringent collaboration plans and disciplined implementations.

Safeguarding critical infrastructure against developing cyber-threats needs a structured approach. It is required that the government aggressively collaborates with public and private sectors on a regular basis to prevent, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation’s critical infrastructure.

It is in demand that the government works with business owners and operators to reinforce their services and groups by sharing cyber and other threat information.

A common platform should be shared with the users to submit comments and ideas, which can be worked together to build a tougher foundation for securing and protecting critical infrastructures.

The government of USA has passed an executive order "Improving Critical Infrastructure Cybersecurity" in 2013 that prioritizes the management of cybersecurity risk involved in the delivery of critical infrastructure services. This Framework provides a common classification and mechanism for organizations to −

- Define their existing cybersecurity bearing,
- Define their objectives for cybersecurity,
- Categorize and prioritize chances for development within the framework of a constant process, and
- Communicate with all the investors about cybersecurity.

Loading [MathJax]/jax/output/HTML-CSS/jax.js