Cyber Security

Aftab Siddiqui

Siddiqui@isoc.org

What is Cyber Security?

Definition

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. [Digital Guardian]

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. [Kaspersky]

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. [Cisco]

Cyber Security

Cyber Security is an overarching term that is used in different context to many or all of the following:

- Information technology and computer security
- Internet infrastructure security
- Security of data, applications and communications,
- Safety of the Internet users

Cyber Security

In the Cyber Security discussions that take place in the various policy fora around the world, there is often little appreciation that the security of the Internet is a distributed responsibility, where many stakeholders take action.

By design, the Internet is a distributed system with no central core or point of control. Instead, Internet security is achieved by collaboration where multiple companies, organizations, governments, and individuals take action to improve the security and trustworthiness of the Internet – so that it is **open, secure, and available to all.**

https://www.internetsociety.org/resources/doc/2020/major-initiatives-in-cybersecurity/

Cyber Security

Internet security is the part of cybersecurity that, broadly speaking, relates to the security of Internet infrastructure, the devices connected to it, and the technical building blocks from which applications and platforms are built.

Cyber Security

In order to understand where security concerns reside, one must of course first survey **vulnerabilities** - existing and potential - within the network or system. A main subject in the study of cybersecurity is **information technology (IT) risk management.**

The **Certified Information Systems Auditor (CISA)**, a widely-recognized accreditation program for IT security professionals, defines risk management as:[4]

> *The process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.*

Assessing risk means taking threats and vulnerabilities into account, determining the likelihood of such events, and projecting their potential impact on the network.

The following is a common formula used for risk:

Risk = Threat x Vulnerability x Consequence

Theoretically speaking, reducing any of the three variables will lower risk, and bringing one variable down to zero eliminates risk.

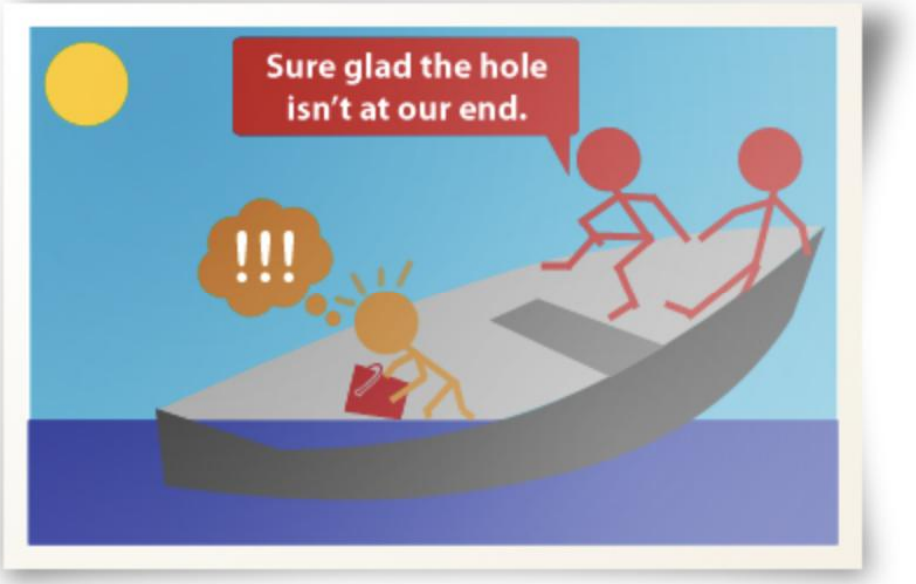
While the practical application of this formula may be difficult (for example, quantifying the variables themselves, or actually eliminating a variable), it is a helpful conceptual model with which to begin when developing a cybersecurity strategy.

Cyber Security

Private firms, as well as governments, undertake risk management to prevent security breaches within their own systems and networks.

But given the interconnectedness of the **Internet ecosystem**, security breaches or a failure to secure one's own systems and networks can also impact others on the outside.

> *Security and resilience of the Internet depends not only on how well risks to an organization and its [own] assets are managed, but also…on the recognition and management of risks that the organization itself, by its action or its inaction, presents to the [broader] Internet ecosystem.*[5]



Collaboration and Coordination

In the national context, and especially in the international context, there is **no single institution** charged with management all of cybersecurity.

As evidenced in the previous section, shared risk management requires collaboration and coordination between multiple actors.

Coordination through:

- public-private partnerships;
- technical assistance; and
- with international law enforcement cooperation;

are just three important examples of the collaboration and coordination that is required on cybersecurity issues.

Collaboration and Coordination

Common Understanding of Solutions

The challenge here is that there is a whole array of possible solutions (e.g. technical, policy, economic, social, etc) and each of them solves only part or one set of the problems at a particular point in time.

It is important to understand that there is no 'silver bullet', but rather, evolving building blocks that can be used in constructing a security solution.

Ability to Assess Risks

The adequate selection of tools and approaches is dependent on the ability to properly assess risks, both **'inward'** as well as **'outward'.** This requires agreement on metrics and factual data, and on the trends associated with them.

This data is also important to measure the effectiveness and impact of such tools once they are deployed, and to monitor the changing dynamics of the environment.

Understanding of Common and Individual Costs/Benefits

The technology building blocks vary in the costs and the benefits they bring to an individual participant and to the common good of the global infrastructure.

Understanding these factors and how they are aligned with the business objectives of network operators and others is crucial for sustained improvements in security and resilience.

Public Private Partnerships

Much of the Internet infrastructure is managed and driven by the private sector; therefore, coordination between the Government and the private sector is essential to building a robust policy approach to cybersecurity management.

It would be a mistake, however, to restrict the Internet policy issues associated with cybersecurity only to these two groups, both broadly defined.

As discussed throughout this module, an open, multistakeholder approach to the development of Internet Governance and policy yields the highest quality solutions.

The Dutch Cyber Security Council, for example:

> *has 15 members from government, industry, and the scientific community, for a total of three scientists, six public sector and six private sector representatives.*[14]

Collaboration and coordination between members of the private sector, the government, as well as the technical community and civil society, has proved essential to developing a fully-informed response to national cybersecurity threats.

Public Private Partnerships

Internet Core Services

Routing Infrastructure

The routing system that interconnects the Internet's tens of thousands of networks needs a secure foundation in order to improve its reliability. Example projects: working groups at the Internet Engineering Task Force (IETF) that work on BGP and RPKI, US National Institute of Science and Technology (NIST), and international Internet Routing Registries (IRR) are working to add security to existing protocols, define industry and government best practices, and create distributed databases that can be used to verify routing information for the entire Internet.

DNS Infrastructure

DNS translates human-friendly names into Internet addresses. A scalable and trustworthy DNS are required by every Internet user. Example actors: DNS Root Server Operators (root-servers.org), Internet Assigned Numbers Authority (IANA), and software developers like Internet Systems Corporation (ISC) and NLnet Labs are all involved in deploying a more secure DNS (DNSSEC), coordinating operation of all DNS root servers, and ensuring secure management of the DNS hierarchy.

Public Private Partnerships

Internet Core Services

Data Communications Security

Encryption of Internet Communications is a basic building block, ensuring privacy of personal and business data. Maintaining the protocols and selecting appropriate encryption algorithms is mainly handled by the IETF and US NIST, in cooperation with international government agencies and a community of hundreds of experts from academia, the public, and the private sector.

Time Infrastructure

Accurate and synchronized time information is needed both within the Internet's cryptographic foundation and in many business applications, such as equities trading. Example projects: International Association of Electrical and Electronics Engineers (IEEE) 1588 and IETF Network Time Protocol working groups are defining new standardized security mechanisms for time synchronization as well as operational best practices for everyone.

Public Private Partnerships

ENTERPRISES, PUBLIC AND PRIVATE ORGANIZATIONS

Wireless LAN Security

The wide use of wireless LANs worldwide calls for strong security against eavesdropping and intrusions. The IEEE 802 Committee and industry groups such as the Wi-Fi Alliance are continuing to advance the state-of-the-art in protecting wireless LAN communications.

End User Device Hardware

Malicious software such as viruses and Trojan horses has caused billions of dollars of losses. The Trusted Computing Group (TCG) and Unified Extensible Firmware Interface (UEFI) Forum have developed hardware-based security such as a Trusted Platform Module and Secure Boot Environments to help combat specific types of malware.

Corporate and Enterprise Security

Common frameworks for information security management systems and best practices help organizations worldwide to meet agreed-upon standards, analogous to common accounting standards such as GAAP and IFRS. Standards such as International Organization for Standardization (ISO) 27000-series and US NIST's SP800-53 series give organizations of all sizes a head-start in improving business information security.

Public Private Partnerships

EMAIL and Messaging

Email (Spam/Viruses/Phishing)

Email is a major vector for cyber-criminals to endanger individuals and organizations with ransomware, stolen credentials, and lost data. Example projects: Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) and IETF email working groups are refining security standards for email, such as Domain-Keys Identified Mail (DKIM), along with best practices such as Domain-based Message Authentication, Reporting and Conformance (DMARC) to counter threats such as phishing.

TRACKING OF THREATS

Immediate operational security threats create chaos when InfoSec professionals are working without good information. A consortium of more than 90 organizations and software publishers, coordinated by MERIT in the US, publishes the Common Vulnerabilities and Exploits database that is used across the cybersecurity community as a basis for defining and fighting current threats. Groups such as the Forum of Incident Response and Security Teams (FIRST), US Infraguard, and private companies such as Verizon, Symantec, and Microsoft regularly collect and freely disseminate security information

IDENTITY

The proliferation of different accounts and passwords creates security and trust problems across the Internet. Identity services help users to carry a single identity with them. Groups such as the Fast Identity Online (FIDO) Alliance and the Open ID Foundation are working to improve security and privacy both for end users and web site operators.

Thank you.

Aftab Siddiqui

Siddiqui@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120