ASM Technologies Limited

Introduction to Cyber Security

Executive Summary

Over the years, the term **Cyber Security** has gained much importance and become a common part of each one's life who is associated with a computer or a smartphone device. When people submit their data online, it becomes vulnerable to cyber-attacks or cyber-crimes. Moreover, cyber-attacks can happen over an external facing DNS server or an internal firewall, which in turn effects the data and infrastructure within the enterprise that inherently causes significant damage to the business of the associated organization.

Cyber Security offers security, from unauthorized access or exploitation, through online services to the massive data, associated appliances and network that is used for communication. The Cyber Security Life Cycle is classified in to various phases.

This white paper summarizes the importance of Cyber Security; how can it be achieved and key points to consider while opting for a Cyber Security service provider.

Types of Cyber-Crimes

- Hacking or illegal access and interception
- Virus
- Malware
- Trojan Horses

What is Cyber Security?

Cyber Security involves protecting key information and devices from cyber threats. It is a critical part of companies that collect and maintain huge databases of customer information, social platforms where personal information are submitted and government organizations where secret, political and defense information are involved. It describes how personal and key government data is protected against vulnerable attacks that possess threat to important information, may it be on the cloud, across various applications, networks and devices. Lot of money are invested in protecting all this information in an online platform. With the number of people accessing the information online increasing each day, threats to the information are also increasing, with the cost of online crimes estimated in billions.

Below is an image showing the top 20 countries with appropriate cybercrime percentage levels.

©Copyright 2017 ASM Technologies Ltd. – All rights reserved.

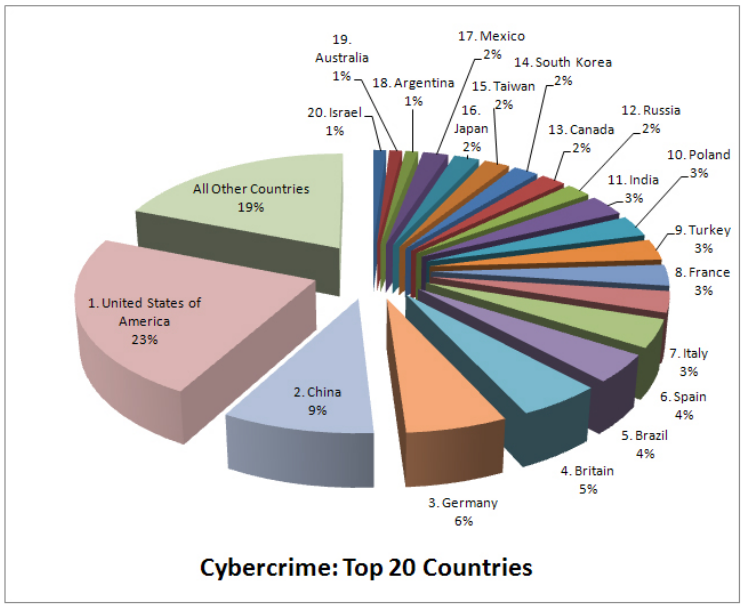

Image source: Google

Security Tips

- **Encryption**: Always use SSL (Secure Socket Layer) to encrypt the data that is transmitted through the internet.
- **Remote Connection**: Use VPN to access remote systems.
- **Software**: Use Anti-virus software.
- **Firewalls**: Install firewalls and pop-up blockers.
- **Uninstall**: Uninstall unnecessary software.

Types of Cyber Security

Cyber Security is classified into the following:

- **Information security** – Information security protects your information from unauthorized access, identity theft and protects the privacy of information and hardware that use, store and transmit data. *Examples of Information security*: *Authorization of user and Cryptography*.
- **Network security** – Network security protects the usability, integrity and safety of a network, associated components, connection and information shared over the network. When you secure a network, potential threats are identified and nullified from entering or spreading on the network. *Examples of Network Security: Anti-virus and anti-spyware, using Firewall to block unauthorized access to your network and using Virtual Private Networks (VPNs) for a secure remote access.*
- **Application security** – Application security protects applications from threats that occur due to the flaws in application design, development, installation, upgrade or maintenance phases.

©Copyright 2017 ASM Technologies Ltd. – All rights reserved.

Choosing the right Cyber Security Service Provider

The best approach to choosing the appropriate service provider requires plenty of foresight and planning in advance. Always compare your needs with the services offered by the software provider.

With various options available in the market, you can choose the right software to protect your data, application, network and the system. You can either opt for an individual service to protect a specific component or use a software that provides a complete solution for all your needs. It is also important to update your applications as and when an upgrade version of the software is available.

Choosing the right service provider can provide you a variety of options to secure your data, applications, hardware and network. Involvement and coordination of the entire business organization is very much important to combat cyber-attacks and efficiently improve cyber resilience using a comprehensive cyber security program. The service provider will be able to assess your organization for your needs and respond to you in various security breaches.

ASM is equipped with top-notch and latest technologies to combat against emerging cyber threats. ASM offers services for developing, documenting, and testing Cyber Security applications. ASM's proven continual expertise in networking makes it one of the best choices to provide a complete set of applications to detect, protect, respond and restore services for various customer types. For more information, refer to our website at http://asmltd.com/.

Our key capabilities include:

- Core managed services include**: Security Banners to authorize users, DNS Blacklists and Integrity Checks, and Access Control (Named ACLs).**
- Advanced security services include**: Threat Insight, Advanced DNS Protection and Firewall, and Security Ecosystem.**

Conclusions

To summarize, information is a critical part of any organization and investing on the right service provider keeps your business in safe hands in the ever-expanding **IoT** (Internet of Things) world. A scalable and customized cyber security-driven business model includes disaster-recovery capabilities and secures data and the underlying infrastructure of the organization, thus building a safe barrier for the information even before it is attacked and saving the organization from a loss of billions of dollars that could result from the security threat.

©Copyright 2017 ASM Technologies Ltd. – All rights reserved.