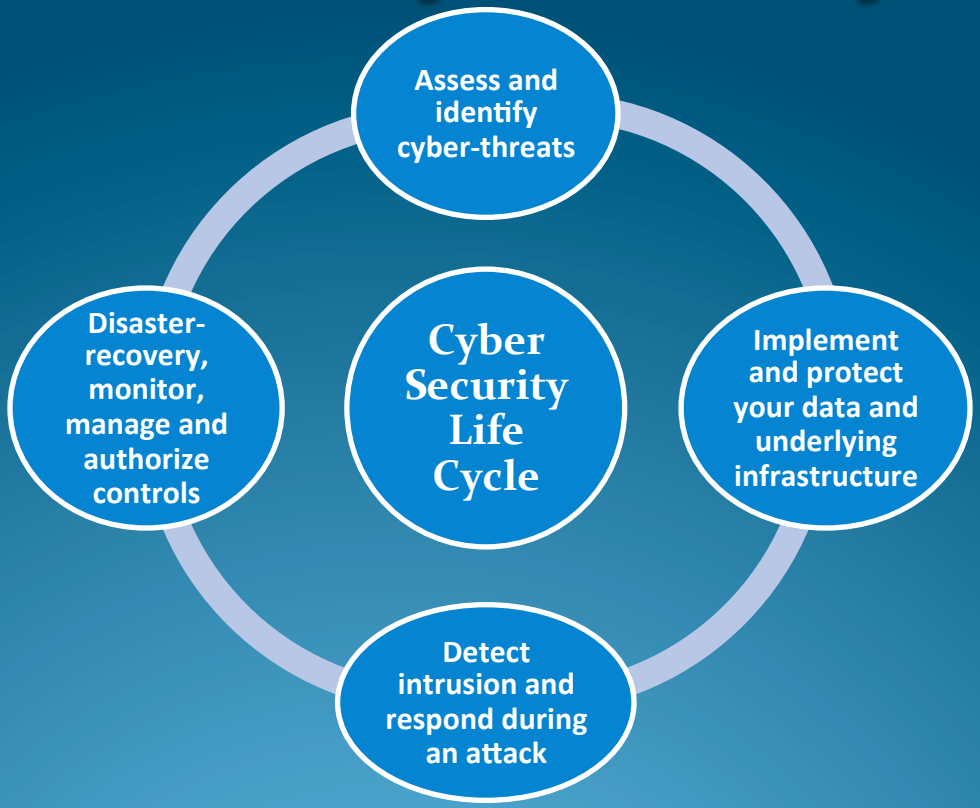
# What is Cyber Security?

Cyber Security protects your key information and secures your network, systems, smart phones, underlying infrastructure and associated applications.

# Why is it important?

If you do not secure your data and the underlying infrastructure, i.e, network, associated systems and applications, your organization is vulnerable to attack from ethical hackers, virus, trojan horses, malware and unauthorized access.

# Cyber Security Life Cycle



# How can we at ASM help you?

We offer the following solutions:

**Core managed services**

- Security Banners
- DNS Blacklists and Integrity Checks
- Access Control (Named ACLs)

# How can we at ASM help you?

We offer the following solutions:

**Advanced security services**

- Threat Insight
- Advanced DNS Protection
- DNS Firewall
- Security Ecosystem

# Security Banners

Create a customized **consent banner** that becomes the first screen of your application with specific terms and conditions that your end users must accept before they login. This way you can permit only authorized users to log in and access your application.

# Security Ecosystem

**Security Ecosystem** comprises of integrated RPZs to detect malware and APTs and TAXII (Trusted Automated eXchange of Indicator Information) service to nullify cyber-threats and attacks.

# Threat Insight

Secure your network from data exfiltration via DNS using **Threat Insight**. The applications that are used to forward IPv4 traffic through DNS servers are vulnerable to DNS tunneling attacks by malware infected devices or malicious insiders.

# Advanced DNS Protection

Configure your own rules, both hardware and software, to detect, report and stop DNS attacks such as DDoS, DNS hijacking, Network-Flood, etc using **Advanced DNS Protection**.

# DNS Firewall

Configure your own **RPZ (Response Policy Zones)** and **define rules** to block malicious hosts. You can also redirect your clients to a  predefined host when a malware or APT (Advanced Persistent Threat) is detected.

# DNS Blacklists and Integrity Checks

- Prevent your users from accessing certain web sites or internet resources by forbidding a recursive DNS server from resolving queries for domain names that are blacklisted using **DNS Blacklists**. You can choose to display to the users that the domain lookup failed due to certain policies or redirect queries to predefined set of IP addresses.
- Protect your authoritative DNS servers from **domain hijacking** using **Integrity checks** by configuring the appliance to monitor DNS records and glue records periodically for top-level authoritative zones and avoid domain hijacking.

# Access Control (Named ACLs)

- Grant access to your hosts for specific operations only using an **ACL** (Access Control List).
- Grant access to your hosts for multiple operations using a **Named ACL** (Access Control List).

# Key Takeaways

- Proven expertise in top-notch technologies to deliver ***a full-fledged best-in-class customizable Cyber Security solution*** that meets customer requirements and delivers result by securing critical information, network, appliances and associated applications of an organization.
- ASM believes in delivering a ***'Go The Extra Mile' Customer Support*** that offers round-the-clock support to its customers beginning from the implementation and throughout the maintenance phase.
- ***Reduced product cost*** and ***quality product*** with ***a user-friendly interface*** that provides an easy-approach to anyone who is using the software. Necessary ***training to resources*** who are going to be associated with the software in-and-out.

# Thank You!