MSS – Managed Security Services and
GISPM – Global Information Security Project Management

by Dipl. Ing. Dr. Bernhard Bowitz
CISSP,AISP,CISA,CISM,MCP,ISO27001,BSI cert.

What is / are Global Information Security Threats to be managed by MSS

- Network and Application Layer Attacks
- Social Engineering Advanced Persistent Threats
- Organized Cybercrime
- Disruption or suspension of servers and network resources connected to the Internet
- Easy attack for anyone to launch, very difficult for enterprises to resolve on their own
- DDoS attack packages readily available to anyone on the black market
- DDoS attacks may be launched by cyber criminals to distract enterprise personnel from noticing fraudulent transactions such as unauthorized data transfers
  Also Called: Denial of Service (DoS) or Distributed Denial of Service (DDoS)
  Frequency: Very Common

Enterprises are frequently targeted by phishing attacks.

- Users receive spoofed (fake) emails used to acquire access to their accounts or acquire personally identifying information
- Fake emails are carefully written to mirror actual emails normally sent out
- Difficult to detect, as the email source often appears legitimate. Also Called: Phishing or Spear Phishing
  Frequency: Very Common

"Backdoor" to your systems is established using vulnerabilities

- Gather administrative credentials and ex-filtrate valuable data
- Using custom malicious code, attackers remain undetected for as long as possible to continue to do damage.
  Also Called: APT
  Frequency: Increasing Every Year

Risk of intellectual property theft

- copy user accounts
- loss of customers as a result of business disruption
- Ultimately easier to prevent than to fix

cyber criminals specialize in selling personal information on the black market

- using ransoms and blackmail
- The BSI, FBI and other Cyber Crime Investigators for example collaborate in investigating and fighting cybercrimes that target i.e. financial institutions, Telecom Providers, Chemical Companies, Governments etc.
  Also Called: Cybercrime Syndicates
  Frequency: On The Rise

Major Data Breaches

- Highly organized hackers using robust infrastructure to target enterprises

- steal customer data and sell stolen data
- Through a variety of methods, sensitive information about enterprises and their customers is exposed
- Business is disrupted
- customer and company data is compromised
- Firewalls, Hardware intrusions, Software Firewalls (NGFW) malware, Administrators
- recovery costs are enormous.
  Also Called: Hacked, Accidentally Published, Poor Security, Lost/Stolen Data, Inside Job
  Frequency: In The News Every Month
  Threats rising

Cyber security breaches are more common now than they have ever been. While they don't all make news headlines, they affect numerous enterprises every single day.

Cloud Security (such as Microsoft Azure, AWS, HPE…)

- Developing Security Concepts for Cloud infrastructures including an abstraction layer that virtualizes resources and logically presents them to users through application program interfaces and API-enabled command-line or graphical interfaces
- **ESA – enterprise security architecture** - cloud computing architecture, cloud infrastructure migrating back-end components - the hardware elements within an enterprise data center
- These include multi-socket, multi-core servers, persistent storage and local area network equipment, such as switches and routers, in a MNC environment
- working with Cloud Security, Microsoft Azure, AWS, NetApp, HPE
- Building a typical Cloud Infrastructure – Secure Computing Infrastructure – Platform and Storage Infrastructure – Applications and Services – Cloud Clients

Mobile Security and Device Management

- With a Secure Device Manager, you manage and control your mobile devices centrally and purposefully
- Safety guidelines uniformly enforced
- Lock devices on loss and remotely delete sensitive data
- Lock web sites and native features such as the camera
- Central setup and push of VPN
- Accesses and emails administration
- E-mail and WiFi access to the device
- Exclude endangered devices from accessing company emails
- Manage apps
- White and blacklisting of apps
- Respond to Apps Policy violations
- Book and identify via a SIM card
- Battery-free virus protection without additional software on the mobile device
- Protection against viruses and malware

Telephone Security Mobile and fixed lines

- App-based voice encryption (Voice-over-IP)
- Secure text messages
- Suitable for smart phones and VoIP of various mobile platforms
- Free use of the service independent of the service provider

- Independent of the carrier's data mode (EDGE, 3G, 4G, WiFi)
- Can also be used abroad
- Even in the WiFi / Wlan networks globally under the own number securely available
- Secure calls End to End between all companies
- Temporary invitation from, for example, project teams or external employees by Administrators

What exactly are these threats?

- How are they carried out and how can they impact costumer and user confidence you should know about
- Solution: A Global Information Security Manager
- A Global Information Security Project Manager **(GISPM)** will be responsible for initiating and delivering the information security projects for an enterprise globally
- Managing Information Security projects adhering to scope, budget and schedule in order to improve an enterprises information security position
- Developing a cloud infrastructure security process
- Working with the division head to execute projects based on the budgeted activities
- Managing the projects of the enterprise globally
- Leading the regional teams to make sure that the global projects are delivered in all regions successfully
- Assessing situations to determine the importance, urgency and risks, and make clear decisions which are timely and in the best interests of the organization
- Leading project teams distributed in different geographic locations
- Travelling globally as per the needs of the projects
- Working with teams/stakeholders in different time-zones
- Working with the lead Security Manager to understand overall global project and the activities to be performed regionally
- Coordinating the regional activities and making sure that those are delivered as per the global schedule
- Reporting regional status, issues and risks to the IT management (on CEO level) on a timely basis
- Travelling regionally as per the needs of the projects

Counter measurements for all current operating systems

- Virus profiles are automatically kept up-to-date in the network
- Protection against the latest standards is ensured
- Centrally hosted in a certified data center

Responsibilities of a GISPM defining and planning the project:
These activities are driven by the IT globally with the support/input from the regional IT management

- Scoping the project and outlining the work to be done
- Calculating the budget
- Determining required resources and ensuring that their roles and responsibilities are clear
- Calculating the schedule
- Creating an ISMS
- The Information Security Management System (ISMS) is a set of procedures and rules within a company that are used to permanently define, control, control, maintain and continually improve information security
- NOC- Network Operation Center 24x7

- SOC- Security Operation Center 24x7

Executing the project:

- Assigning the tasks to the resources
- Ensuring the execution of the global tasks by the respective team members
- Coordinating the execution of the regional tasks with the regional project managers
- Resolving any arising conflicts and issues on a timely manner

Controlling the project

- Monitoring the progress of the project and making adjustments as necessary to ensure the successful completion of the project
- Keeping the respective division head and key stakeholders informed of the project progress, risks, issues and mitigating controls
- Monitoring all budgeted project expenditures
- Ensuring that all financial records for the project are up to date
- Ensuring that the project deliverables are on time, within budget and at the required level of quality
- Ensuring that all project information and or decisions are appropriately documented and secured

Closing the project

- Evaluating the outcome of the project and communicating this to the management and to the key stakeholders
- Ensuring smooth handover to the respective teams
- Gathering lessons learnt and using those to improve the process for the future projects, train the local teams

A suitable MSS Project Manager must have

- Certifications for example: CISSP,AISP,CISA,CISM,MCP,ISO27001,BSI GRUNDSCHUTZ, PhD
- Additionally shall have BS/MS in a discipline with IT focus degree
- Minimum 10 years of Project Management experience
- Minimum 15 years of IT experience
- Experience in working at international environments
- Demonstrates understanding of information security, web security, network security, anti-malware and risk management
- Experience in creating an effective team environment, building relationships, negotiation, solving problems and issues, resolving conflicts, managing resources in a matrix environment and communicating
- Good planning and organization skills
- Excellent communication skills in English both written and spoken
- German language an advantage, as well other languages
- Judgment and decision making
- Analytical thinking & problem solving
- Management and leadership skills
- Team player
- Good negotiation skills
- Creative thinking
- Technical skills
- Efficient time management
- Taking initiative
- Fast adaptation to new environments
- Stress tolerance
- Ambition and persistence to deliver under challenging conditions
- Comfortable to evolve in a changing environment
- Conflict management

- Understanding of different cultures

Conclusion

Manage all the projects adhering to scope, budget and schedule
Ensure the delivery of the assigned projects adhering to scope, budget and schedule = **MSS / GISPM**