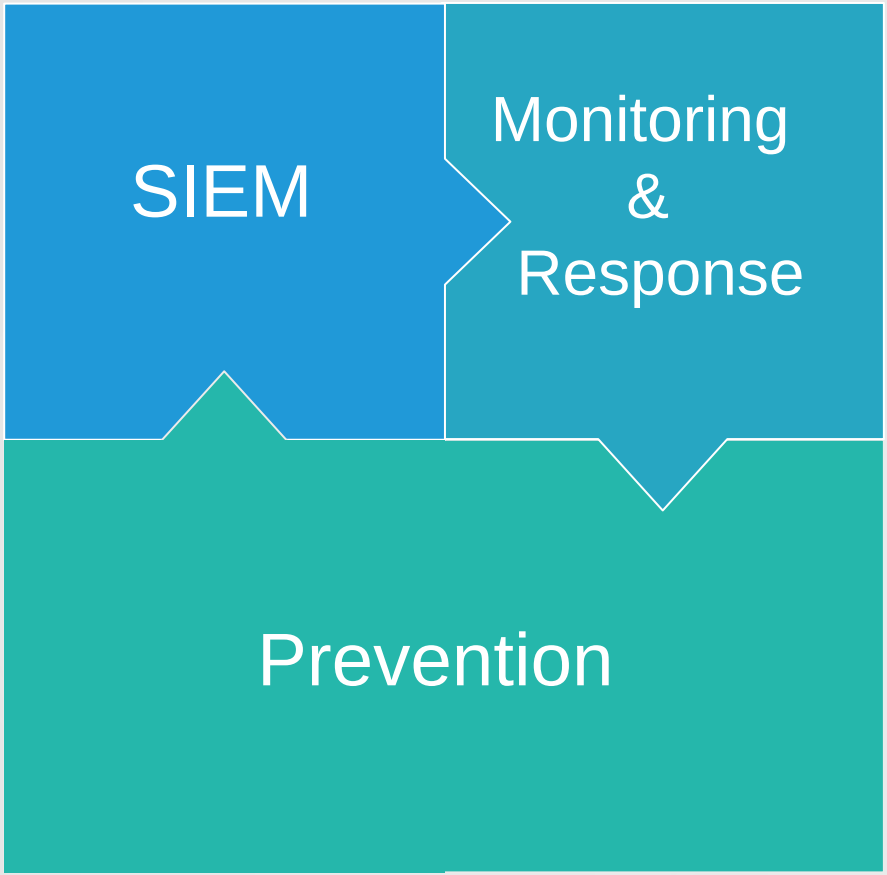
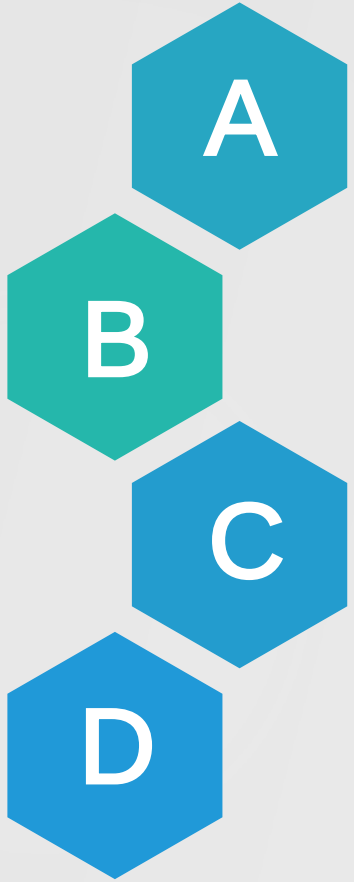
“Managing Security in the New Digital Era”

3rd International Conference
CYpBER2020

SOC Components



Digital Transformation



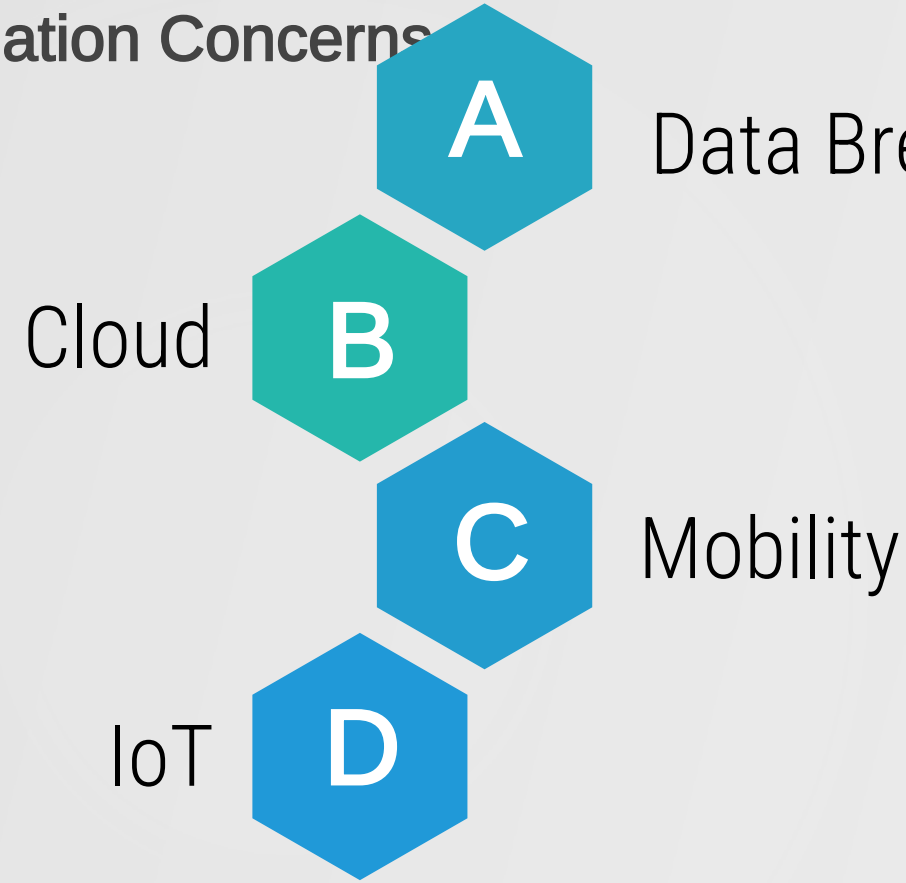
Rising Cybercrime

Digital Disruption

Compliance Demands

Skill Shortages

Digital Transformation Concerns



Critical Infrastructure Attacks

Ukrainian Power Outag

In December 2015 a massive po
and data acquisition (SCADA) c
without power for hours.

The seed of this chaos was sew
is relevant today, with phishing
factor in the success of these si

Precisely a year after this attac
causing an hour long blackout i
question whether these attacks

Eugene Kaspersky, cybersecuri
on the brink of turmoil, with ha

Home › Cyber Security

Share Tweet

A ransomware attack has targeted critical infrastructure
based natural gas compression facility, a statement put o
of Homeland Security (DHS) from February 18 has confir

Portrait photography: Peter Elmholt

Share

Maersk: Springing back from a catastrophic cyber-attack

Rae Ritchie – August 2019

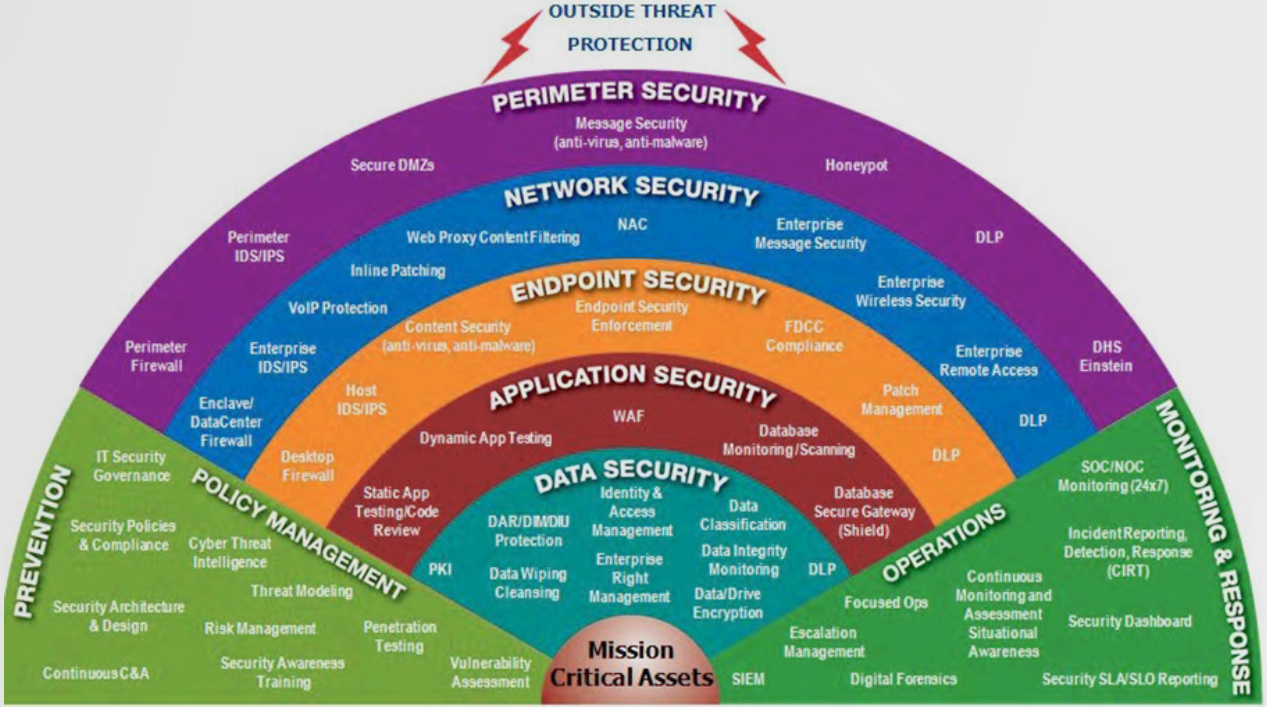
Adam Banks, head of technology at the global transport and logistics giant, shares the inside story of the company's crippling assault by the NotPetya malware — and its astonishing recovery.

It's June 27, 2017. Adam Banks has just returned from honeymoon and is back in his role as chief technology and information officer of Maersk, the Danish transport and logistics giant, best known for its shipping containers.

The Complexity of Cyber Security

- Roughly 45% of malrware gets detected by antivirus software as per the vice-president of Symantec. So what do you do about the other 55%?
- Do you have the necessary controls to prevent infection?
- Do you have the necessary mechanisms to detect malware speading through your network?
- Do you have the necessary procedures and tools to quickly respond and contain the attack?
- Do you have the necessary in-house skills or trusted vendors to help you achieve these?

Layered Cybersecurity Defence Network



Security Hardening & Architecture Design

- Proper network segmentation is a very effective preventive measure that can significantly reduce the impact of attacks.
- Security hardening of operating systems, databases and applications can help keep attackers out of systems.
- Restricting access rights for users to only those resources absolutely required to perform routine activities (principle of Least Privilege).
- Establish a containment model for administrator account privileges (3 tier model)

IT Security Governance

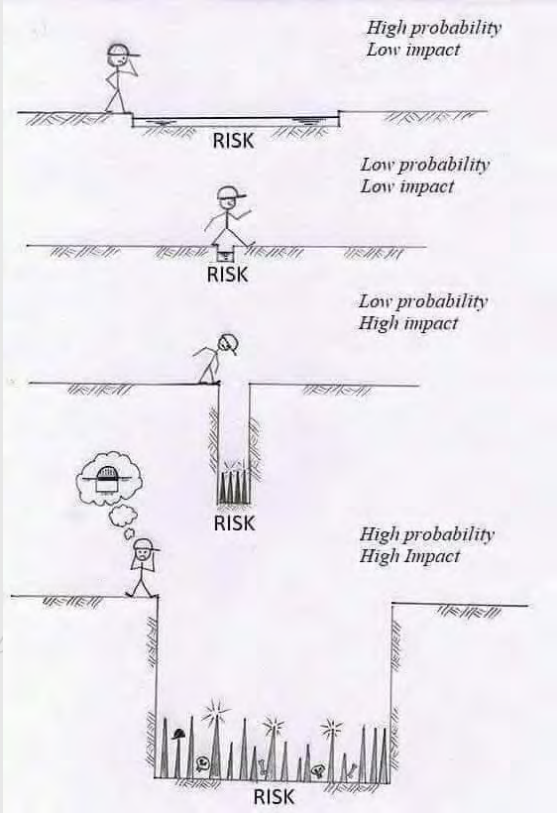
- Written information security policy documents are a formal declaration of management's intent to protect information.
- They outline specific requirements, rules or regulations that must be met.
- They are the foundation upon which all information security related activities, decisions and investments are based.
- It covers areas such as IT operations, security, change management, development processes, and IT governance.
- They are tailored to corporate needs in order to enforce good governance and create a secure environment.

Risk Management

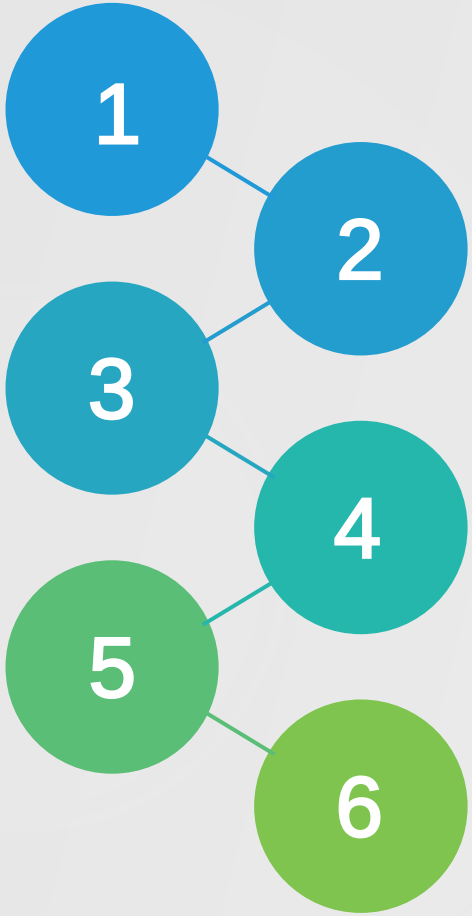
"Risk management is the process of **identifying**, **assessing**, and **controlling** threats to an organization's capital and earnings"

Important Benefits

- Confidence in the business decisions taken
- Creates safe and secure work environment for staff and customers
- Increases the stability of business operations while decreasing legal liability
- Provides protection from events that are detrimental to both the company and the environment
- Protects all involved people and assets from potential harm
- Helps establish the organization's insurance needs in order to save on unnecessary premiums



Risk Management Processes



Establish Context

Understand the circumstances in which the rest of the process will take place. Establish the criteria that will be used to evaluate risk. Define the structure of the analysis

Risk Identification and Analysis

Identify and define potential risks that may negatively influence a specific company process or project. Then determine the odds of them occurring and their consequences.

Risk Assessment and Evaluation

Make decisions on whether the risk is acceptable and whether the company is willing to take it on based on its risk appetite.

Risk Mitigation

Assessment of the highest-ranked risks and develop controls to alleviate them. These controls include risk mitigation processes, risk prevention tactics and contingency plans.

Risk Monitoring

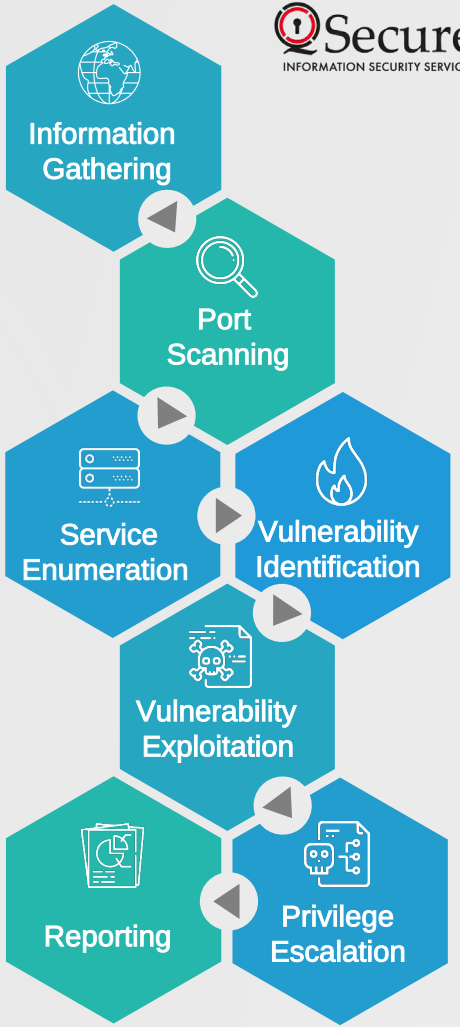
Part of the mitigation plan includes following up on both the risks and the overall plan to continuously monitor and track new and existing risks.

Communication and Consult

Internal and external shareholders should be included in communication and consultation at each appropriate step of the risk management process

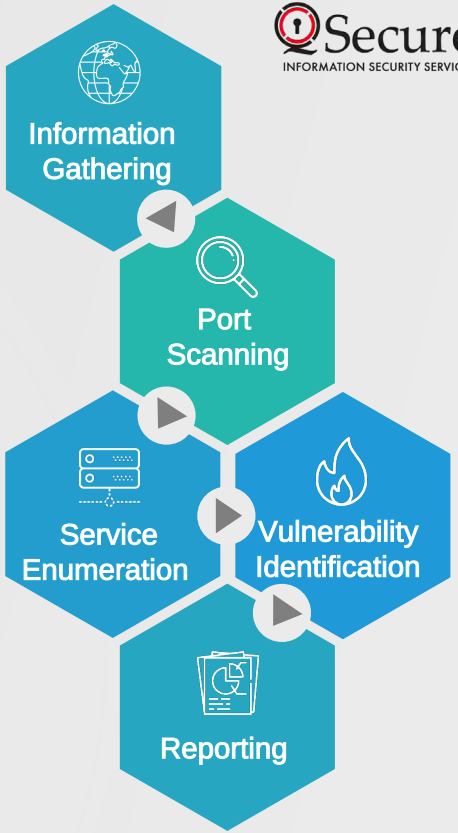
Penetration Testing

- Simulation of real hacker attacks against an organization's perimeter systems.
- Involves the exploitation of identified vulnerabilities in order to show the true impact of a possible hacker attack.
- Includes automated and manual tests.
- Shows the true picture of an organization's security posture as seen from a hacker's perspective.
- QSecure performs simulated hacker attacks as "informed" and "uninformed" attackers.



Vulnerability Assessment

- Is a cheap way to quickly get an idea of how vulnerable your systems are.
- Involves only automated scans. No manual testing is performed. Human logic is not utilized.
- No verification of results is performed hence there is a high probability for false-positives.
- No exploitation of identified vulnerabilities is attempted hence the true impact is not assessed.



Security Awareness Training & Phishing Campaigns

- A well-trained user is considered the last line of defense against social engineering attacks when automated controls have failed.
- Users need to be continuously educated on information security risks and best practices.
- They need to be taught to be suspicious whilst on the Internet.
- The focus should be to achieve a long-term shift in the attitude of employees towards security.
- Frequent testing through phishing campaigns helps keep them alert.

Threat Monitoring

24/7/365 monitoring of compromised and exposed credentials on the Dark Web from various sources, such as:

- Botnets
- Criminal chat rooms
- Peer-to-peer networks
- Malicious websites and blogs
- Bulletin boards
- Illegal black market sites
- Private and public forums

Our Certifications

Thank You

CDMA Services Ltd (QSecure™)

Michael Nicolaou
michalis@cdma.com.cy
+357 22 028 014

QSecure
INFORMATION SECURITY SERVICES