High-Performance IT

Security Health Check

russell futcher .com

The Best practice IT Standard is comprised of:

Six levels of managed security with penetration testing, underpinned by CARTA (a strategic approach to information security that was introduced by Gartner in 2017).

Security levels

1. IT security. Refers to securing digital data, through computer network security. It is accountable for preventing unauthorized access to organizational assets such as computers, networks, and data and it maintains the integrity and privacy of corporate information and the blocking of hackers.
2. Information security, on the other hand, refers to the processes and tools designed to protect business information from unauthorised access.
3. Network security. Used to prevent unauthorized or malicious users from getting into a network, ensures that capacity, reliability, and integrity are not compromised. The Network security risk profile increases as business increase the number of endpoints and migrates services to the public cloud.
4. Endpoint security. Protects mobile phones, laptops, and desktops. It restricts access to malicious and typically includes malware protection and device management.
5. Internet security. The protection of information that is sent and received in browsers. Includes network security involving web-based applications. These protections come in the form of firewalls, anti-malware, and anti-spyware, ransomware.
6. Cloud security. Applications and data held in a cloud-based data centre. The usual security measures do not protect users who are connecting to the internet. Cloud security secures software-as-a-service (SaaS) applications and the public cloud.

CARTA

Within the CARTA approach, decisions and security responses are made based on risk and trust. There are three phases of IT Security where CARTA plays a role: Run, Plan and Build. In the Run phase, CARTA lets the organization use analytics to focus only on the biggest threats and automate the majority of the incidents. In the Build phase, CARTA plays a role in DevSecOps, as teams identify threats and eliminate them from apps they are building and use things like a digital risk rating service to analyse open-source components they may want to use. In the Plan phase, CARTA invites organizations to use analytics to determine the risks of things such as having employees change passwords frequently versus the productivity impact and decide how much risk to accept. (Source, SUSE).

Performance Assessment

- Does your security function cover the five security types?
- Is there a security manager?
- Does the security manager report to the Infrastructure manager?
- Is your security managed in-house, or is it outsourced?
- What types of annual penetration testing takes place?
- What resolution times for new threats are you receiving from your external suppliers?
- What is the number of security violations per month?
- Are the security violations trending upward?
- What are the number of monthly security violations/hacks by security type?

Sample Task list

- Carry out a risk analysis of the five security functions.
- Review all five levels of security for completeness.
- Arrange external penetration testing.
- Define and design a systems security architecture.
- Determine further works required and scope out.
- Breakdown the scope of works to task level, ready for loading into the change management project schedule.