GDPR Update and ENISA guidelines

2016

There are two topics that should be uppermost in every CISO's mind, how to address the growing demand for Unified Communications (UC) and how to ensure that the organisation's compliance obligations are met. Responsibility for compliance extends beyond the CISO to the entire board. These issues are linked because any UC implementation impacts the deploying organisation's compliance status. This white paper examines the UC compliance issues and shows how with the correct security controls, an organisation may realise the benefits of UC without compromising their compliance status.

INFORMATION UPDATE

Introduction

Universal and Real-Time Communication (UC and IOT) compliance, delivered to certify the risk levels and assure Corporates that they will adhere to EU and US based Cyber-attack directives, as set out in 2015 to extend and protect Personal Data.

UM-Labs have worked with various Audit Partner's and more recently Tier One Carriers to add to their Cyber Risk Services. This helps complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation and performance objectives through proactive management of the associated cyber risks.

Deeply experienced across a broad range of industries, these Audit Partner's Cyber Risk Services practitioners, provide advisory and implementation services, spanning executive and technical functions. This helps to transform legacy IT security programs into proactive, secure, vigilant and resilient cyber risk programs that better align security investments with risk priorities, established to improve threat awareness and visibility, and strengthen the ability of organizations to thrive in the face of cyber incidents.

Compliance and assurance means that together with UM-Labs, partners can offer a powerful integrated business and technology solution enabling companies to adequately prepare for and manage the entire life cycle of a cyber-incident. Organizations today need to quickly contain the damage, but they also need a solutions provider that can help them regain full business strength and improve their capacity to withstand future crises. UM Labs makes it possible for your clients to meet tomorrow's cyber challenges head-on while continuing to power performance in their businesses.

IT security is the process of applying security measures to ensure confidentiality, integrity, and availability of data. IT security attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of IT security is to protect data both in transit and at rest. Countermeasures can be put in place in order to increase the security of

data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.

Most organizations have implemented reasonable to adequate technologies to mitigate the IT security risk of traditional network infrastructures. Measures range from classical on-premises endpoint solutions like firewalls and proxy servers to managed security services from the cloud.

With the advent of Universal Communications (UC), a separate Network Data Application, accompanying risks are mistakenly classified following traditional threat tables. It is an unfortunate fact, however, that existing mitigation measures like Session Border Controllers (SBC's), gateways and internet proxies are not able to effectively protect specific UC functionality. SBC's are not designed to protect against modern cyber-attacks. The European Network and Information Security Agency (ENISA) Technical Guideline, which is mandatory for Network Service Providers (NSP) and the services they deliver, shows clearly the mismatches between the legacy gateways such as SBC etc. and their capabilities and the security obligations.

Impact Law and Legislation

In December 2014 and again in 2015, ENISA published a set of technical guidelines, with which an organization can implement processes and security measures that comply with the legislative requirements for the security of electronic communications of the European Union. HR 1770, the Data Security and Breach Notification Act of 2015 in the USA along with the EU Directive EU Directive 95/46/EC in Europe present major milestones for Cyber Security compliance.

The technical guidelines are developed with the aim to provide for a standardized framework for mobile networks, VoIP and UC solutions. They take technical and organizational measures into account. These guidelines indicate, amongst others, that the deployment of SBC's for UC solutions do not comply with the EU legislation. The technology for UC solutions applied by UM Labs, however, provides 100% compliancy with these regulations.

Security & Assurance from UM Labs

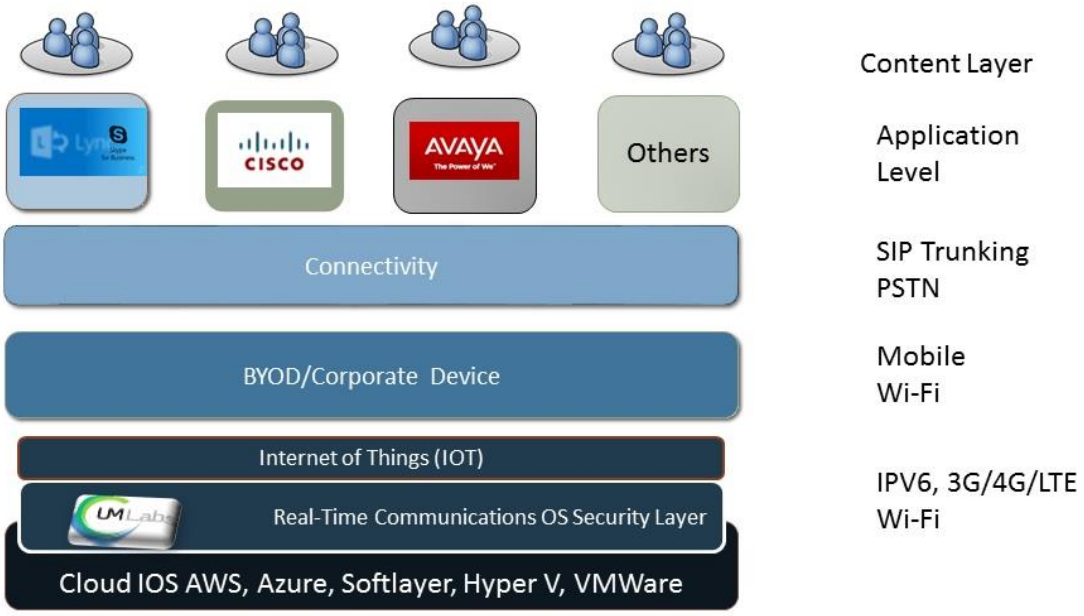
UM-Labs R&D have provided a platform designed for the 21st century and in this our partners can provide the UC IaaS services to deliver an ISO27001 certificate.

The 27001 certificate proves for their customers that the Security Management process is under control. The Statement of Applicability is based on a service specific risk analysis.

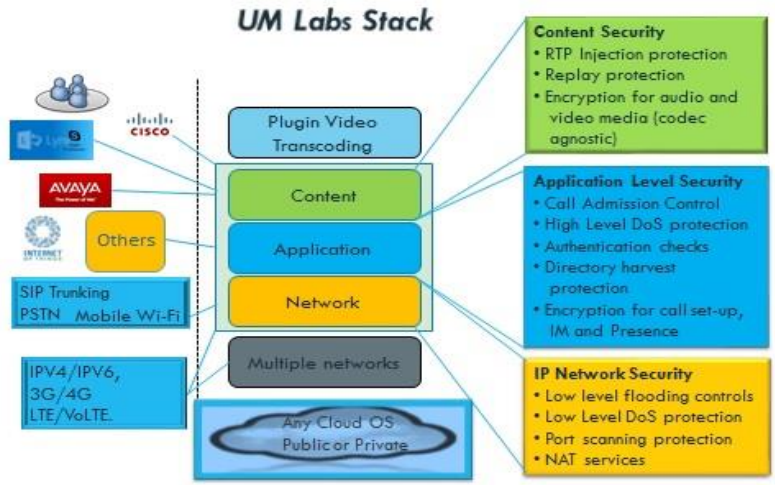
Besides ISO27001 and to be introduced ISO28000 for inter-op between platforms, the service will also be subject to an assurance statement based on the ISAE 3000 range (ISAE3000 or ISAE3402).

The statement is a type II statement which describes the design, existence and effectiveness of the controls. An independent (third party) auditor will create the statement. The NSP partner Compliance Framework will be the basis for the provided ISAE statement.

The partner is free to combine the ISO certificate with the ISAE statement. Optionally, the ISAE statement can be shared and discussed with customers.



Delivered as a software layer OS to protect on three layers, network, application and content, fully integrated to protect from multiple attacks.



Call to action

As the new global regulation and legacy architecture for network and cyber security are proven to be incompatible with 21st century Cyber-attacks, the move towards filing any gaps in the obvious legacy, becomes urgent. Many suppliers, if not all of, see re-design as a daunting task, it is now being taken on board by them and the result is to merely move old designed hardware products, such as firewalls, SBC's and application gateways into a software defined solution.

This has not created new design for new threats, to achieve compliant and resilient Cyber Security, especially in the real-time communication space, it is imperative there is an integrated multi-layer attack protection that responds at the network, application and content levels, (by way of example, a DOS attack at the network is often used to create disruption so that the next more sophisticated DDOS attack at the application level prevents service use and opens up the single point firewall or proxy and allows hacker access on content.)

UM-Labs R&D have tested against rigorous POC and regulator input to show how the platform running in any cloud provides multi-layer protection by full integration and management of real-time communications, the layered security OS from UM-Labs sits at the point of the Network entry, allowing any access from mobile or desktop into any UC system's, while fully encrypted and delivered on scale, with all known attacks managed, logged and prevented. As an SDN

implementation, designed as a layer, it is easy to update for new attacks and provide, if needed, patches in real-time.

As the solution can run on any cloud (private, public or Hybrid, bare metal if needed), providing security for 100,000 of users within minutes not days or months, it is anticipated this will be acceptable to hosting, NSP and private organisations, making their real-time communications compliant. Just in time!