Liguria Digitale

The Regional Cyber Security Center: Use Cases in Healthcare

Innovating the Healthcare:

Trends, Challenges, Opportunities and Risks

Ing. Sandro Pellerano, Ing. Laura Lo Cicero

CISEF Gaslini Genova, 18 Giugno 2018

Agenda

- Liguria Digitale
- Healthcare data security
- Legal requirements
- Liguria Digitale actions:
  - Control Room Liguria
  - Technological measures
  - Organizational measures

Liguria Digitale

Liguria Digitale is a company totally owned by Regione Liguria (following in-house model) and provides products and innovative solutions for **Public Administrations**, **Healthcare Structures** and **Citizens**.
Our mission is to design, plan, realize and manage **Digital Infrastructure** of our partners and customers and **make this infrastructure secure**.
Liguria Digitale has been taking care of Liguria region Health Information System, with an explicit focus on the related digital and ICT aspects.

Electronic Health Record and paperless prescription

We manage the set of electronic health and social data related to one person.

ICT infrastructure

We collect, secure, manage and process all the information related to the health of individuals living in Liguria and to the activities of the organizations working within the health sector.

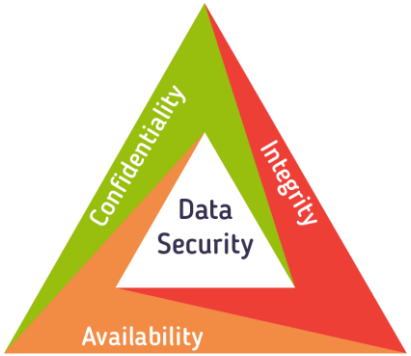
Data storage and backup

We provide storage and data backup for the Local Health Centers (called ASL) and the main hospitals in the region.

Healthcare data security

Healthcare data security isn't just about protecting confidentiality (**sensitive personal data**). When its integrity or availability is compromised, there is a **potential risk for patients**. Whereas up until now, and as far as we know, no data confidentiality breach has ever led to a person's death.

With the **informatization of the hospital's core business**, i.e. healthcare, people started having concerns about security, just like the banking sector did, ten or twenty years earlier.



1. **Integrity**
2. **Availability**
3. **Confidentiality**

GDPR and data breaches

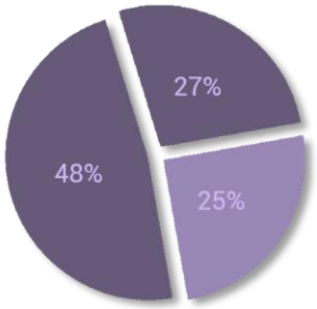
*"A **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"* (GDPR Article 4, Definitions)

Data Breach may result in significant **risks for Privacy**.

The General Data Privacy Regulation (GDPR) of the European Union places an **obligation**, for Public Administration and Companies, **to communicate** a data breach to Data Subjects and Data Protection Authority.

Main causes of data breaches in 2017:

- Criminal Attacks (48%)
- System Gliches (27%)
- Human Errors (25%)



NIS Directive

The **Directive on Security of Network and Information Systems** aims to raise levels of the overall security and resilience of network and information systems across the EU, through:

1. Improved cybersecurity capabilities at national level;
2. Increased EU-level cooperation;
3. Risk management and incident reporting obligations.

Operators of essential services

- Private businesses or public entities with an important role to provide security in:
  - Energy: electricity, oil and gas
  - Transport: air, rail, water and road
  - Banking: credit institutions
  - Financial market infrastructures
  - Health: healthcare settings
  - Water: drinking water supply and distribution
  - Digital infrastructure (IXP, DNS, TLD)

Digital service providers

- Online marketplaces
- Cloud computing services
- Search engines

NIS Directive

Operators of essential services: obligations

The identified operators of essential services will have to take appropriate security measures and to notify serious cyber incidents to the relevant national authority:

Security obligations:

- Preventing risks by taking appropriate security measures
- Ensuring security of network and information systems
- Incident handling

Reporting obligations:

- Notification of incidents having a significant impact on the continuity of the essential services to the competent authority or the CSIRT, without undue delay

Notify substantial incidents to the competent authority:

Number of users affected

Duration of the incident

Geographic spread

Control Room Liguria

Starting from the last months of 2017 Liguria Digitale has realized a **state-of-the-art Control Room** as a collection of technologies and skills in security, systems and network management, monitoring and incident response.

The Control Room is composed by:

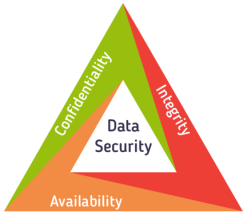
- **Security Operations Centre (SOC)**
- **Network Operations Centre (NOC)**

It has been realized on LD's premises and it is managed by LD's skilled specialists.

Network Operations Center (NOC)

The Network Operations Centre is the central location from which network administrators **manage, control and monitor the networks**.

The overall function is to maintain optimal network operations across a variety of platforms, instruments and communications channels.



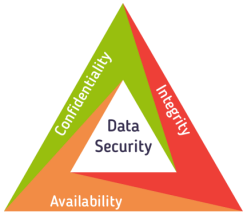
1. Integrity
2. **Availability**
3. Confidentiality

Elements and activities:

- Network monitoring
- Performance and availability of systems and applications
- SLA compliances and downtime limitations
- Data Center Monitoring (temperature, power supply, smoke and water presence)
- Video surveillance

Security Operations Center (SOC)

Liguria Digitale's Security Operations Centre is the centralized unit that deals with **security issues on an organizational and technical level** with tools and solutions for the **prevention and treatment of IT security incidents**.



1. **Integrity**
2. **Availability**
3. **Confidentiality**

Elements and activities:

- Antispam
- Next-Generation Firewall
- Security Information and Event Management (SIEM)
- Endpoint detection and remediation
- Vulnerability assessment / management
- Incident handling
- Computer forensic
- Security policies and procedures

Liguria Digitale

Technological measures

Antispam	Interception of emails containing suspicious content, attachments or URLs, through antivirus and phishing detection technology
Endpoint detection and remediation	Advanced endpoint protection able to detect and apply automatic remediation in case of advanced attacks, zero-day and threats like ransomware, rootkit, trojan, viruses and worms
Next-Generation Firewall	Traditional firewall with other network device filtering functionalities, such as deep packet inspection (DPI) and intrusion prevention system (IPS)
SIEM	Log collection from the IT infrastructure (client, server, network devices, security devices and applications), real-time monitoring and correlation of events in order to identify potential threats and suspicious activities
Vulnerability management	Cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities on systems

Organizational measures

Organizational measures implemented in order to ensure a level of security appropriate to the cyber-risk:

- **Risk analysis** review
- **Incident handling**: Identify, Protect, Detect, Respond and Recover (Cybersecurity Framework 2015)
- Protocol agreement with **Polizia Postale e delle Comunicazioni della Liguria** to prevent cybercrime on critical systems of Regione Liguria (Information sharing, notification of emergencies related to vulnerabilities, threats and incidents, identification of attack sources)
- **Training** and **awareness**
- **Security policies and procedures** in order to develop and complete the Information Security Management System (ISMS)
- Complete **Risk Assessment & Business Continuity** project

Liguria Digitale

Thank you

s.pellerano@liguriadigitale.it

l.locicero@liguriadigitale.it