



**Working Party on  
Land Administration**



DEPARTMENT OF LANDS AND SURVEYS - CYPRUS

**How are land administrations responding to evolving threats to maintain system security?**

**The case of DLS – Cyprus.**

---

**NEOCLIS NEOCLEOUS – CHIEF LANDS OFFICER**

*UNECE WPLA WEBINAR – CYBER SECURITY*

*22<sup>ND</sup> FEBRUARY 2024*



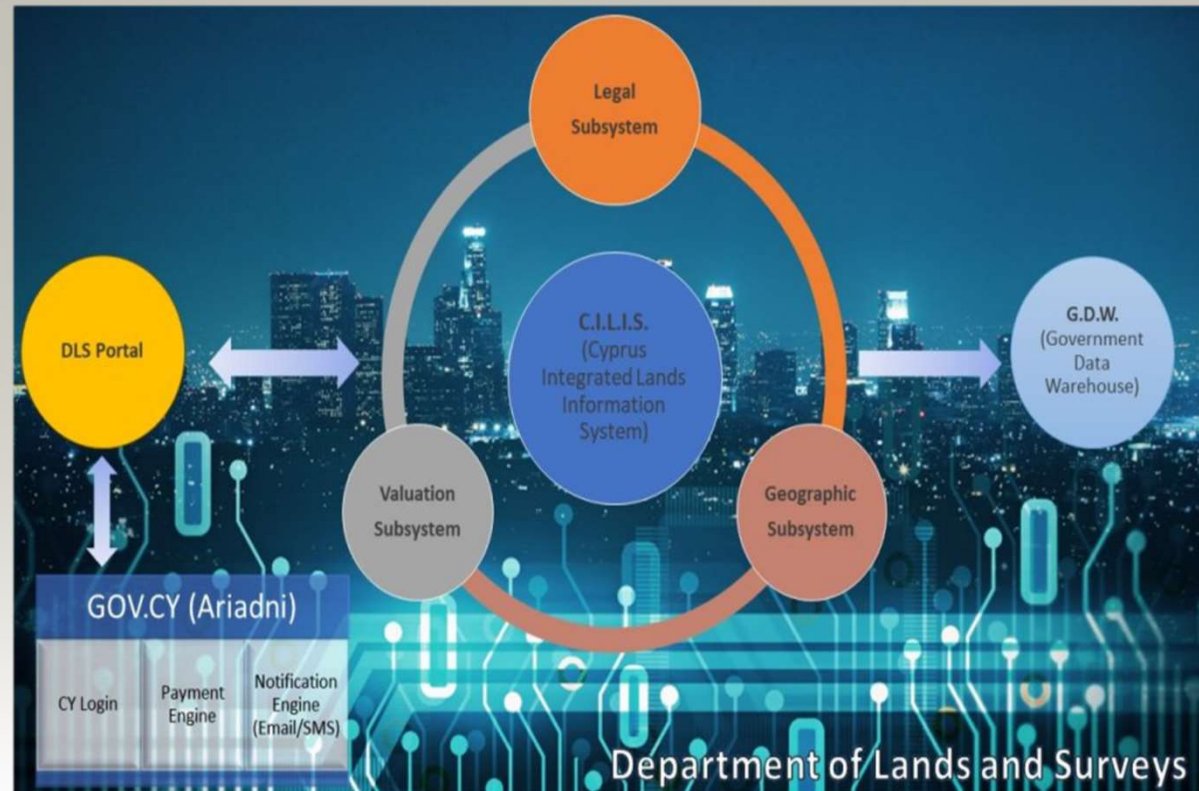
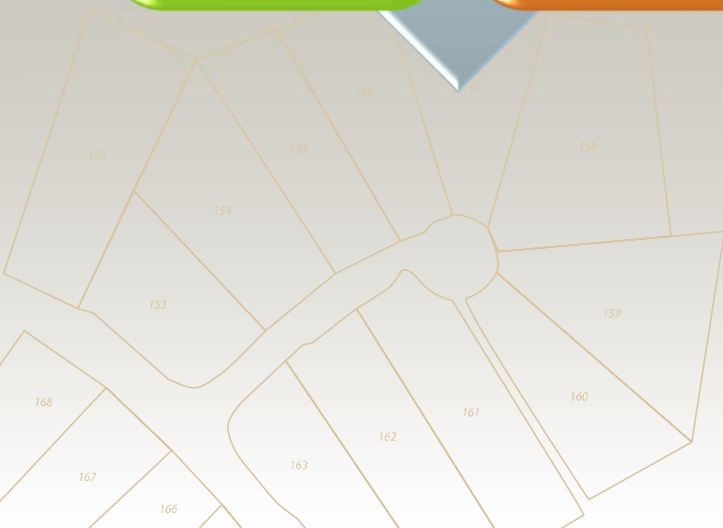
## Department of Lands and Surveys:

### Historical Background:

- i. Ministry of Interior - **1858** started operations*
- ii. Initial Task: Registration of Title*
- iii. Title System - Torrens Based*
- iv. Fixed Boundary System*
- v. Parcel Based / Centric - Unique ID*
- vi. Highly Respectable and Reputable System of Tenure, Registration, Valuation, Cartography, Survey.*
- vii. Efficient / Secure and Multipurpose Cadastre*
- viii. Multitask Umbrella Organization - All Aspects of Land Related Matters Under a Single Roof*



# DLS Additional Facts:





# DLS Evolving Mission THEMES:



## Economic

- Russia's war on Ukraine
- Property vs Cash (Bank)
- Cost of Living Crisis / Inflation
- Banking Crisis
- Foreign Investment in CY
- National GOV Projects Increase



## Regulatory

- New Operating Models - Agile
- Cyber, Fraud & Data
- Operational Resilience
- Consumer / Customer Duty
- Critical Infrastructure
- Laws Amendment – EU -  
eCadastre & eMortgage



## Technology

- Enterprise Solutions
- Old Legacy Systems End
- e-Government Solutions
- New Channels & APIs
- Artificial Intelligence (AI)
- Agility & Cloud
- Data = Strategic Asset



## Customer

- New End-to-End Frictionless Customer Journeys
- The New Digital
- Any Time / Place / Device
- Satisfied Happy Customers
- Time is Precious



## Workforce

- Flexibility / Expectations
- Hybrid Working
- Diversity
- Engagement
- Skills Shortages / Knowledge
- Learning Gap
- 1 Person – 1 End-to-End Process



# Digital Transformation (Evolution) – DLS NICHE:

INTEGRATED LR & CADASTRE (LEGAL / FISCAL / GIS)

IT LEADER IN CYPRUS GOVERNMENT – USED AS A PROTOTYPE

DLS AS A CRITICAL INFRASTRUCTURE

NEARLY 100% DIGITILIZATION

CENTRAL SOURCE OF DATA – DATA IS OUR STRATEGIC ASSET

AGILE MANAGERIAL DECISION MAKING

STRONG DLS VISION - THINK OF WHAT PEOPLE TODAY DEMAND!

**EMBRACEMENT OF CHANGE**

GIVE PRACTICAL SOLUTIONS TO COMPLEX PROBLEMS!

NATIONAL GOALS / PROJECTS FACILITATOR

ECOSYSTEM OF SECURITY





# Digital Transformation – Latest Large IT Applications:

3 Mass Valuation Projects (2013/2018/2023) – Digitally – Integrated GIS Project

DLS Portal / e-Apps (30+) & Map Navigation / 200+ Layers of GIS Info

Data as an Asset – All DLS Data Served Horizontally in the Government

Mass Mortgage Transfers for Systemic Banks – 1 Day Process !

Enterprise GIS – Latest Technologies – Parcel Fabric

2024 – LEGAL / FISCAL UPGRADE PROJECT









# The “DLS PORTAL”:







## DLS PORTAL:

### Latest Statistics - 2023:

- i. No of e-Applications: **200.000!***
- ii. Parcel Navigation Visits: **10 Million!***

***"Considered as the No. 1 Property Platform!"***  
***Property Investors Facilitator!***



## DLS DIGITAL TRANSFORMATION NICHE PILLARS

### DATA

Completeness  
Accuracy  
Validity  
Reuse

### PROCESSES

Simplicity  
Reengineering  
Break Down Silos  
Transparency

**BUILT IN INTO YOUR IT SYSTEM**

DLS Title System  
Land Tenure  
Integrated Cadastre

### INFRASTRUCTURE

Hardware / Software  
Best Practices  
Security  
Governance

### HUMAN RESOURCES

Dynamic  
Agile  
Continuous  
Essential Part of the Vision  
& Culture Change







# TERMS & FACTS CYBER SECURITY



## Cyber Security:

### Important Terms:

- **Cyber:** *"refers to both information and communications networks."*
- **Security:** *"The state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured."*



## Cyber Security:

### Important Terms:

- **Cyber Security:** *"the body of technology, process, and practice, designed to protect systems, networks, programs, and data from cyber risks like cyber-attacks, damage, or unauthorized access. It is also referred to as information technology security."*



## Cyber Security:

### Important Terms:

- **Threats:** "An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss."
- **Adversary ('threat source'):** "Person, group, organization, or government that conducts or has the intent to conduct detrimental activities."
- **Vulnerability:** "a flaw or weakness that may allow harm to occur to an IT system or activity."



## Cyber Security:

# Important Terms:

### Event

- Any observable occurrence within a system.
- Successful or unsuccessful attempt, intentional or accidental
- Doesn't necessarily pose a threat, but it warrants monitoring and investigation

### Incident

- Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- Indicates an attempt to compromise security or actual harm caused

### Breach

- Specific type of incident where there is a confirmed disclosure of information to an unauthorized party
- It's the culmination of an incident where attackers achieve their malicious intent
- Are significant security failures, as they involve the loss of control or unauthorized access to sensitive, protected, or confidential data



## Cyber Security:

### Important Facts:

- *Cyber-security is not so much about exotic and esoteric hacking attacks (the stuff of movies)*
- *It's not always about bad guys, or about technology!*
- *>70% of security breaches occur within the organization*
- *>99% of attacks are opportunistic and random, not targeted*
- *Most cyber-attacks can take place because of operational lapses and deficiencies*
- *Hackers know we have protection technologies today so they find weaknesses, errors and loopholes to try to come in by*



## Cyber Security:

### Important Facts:

- *Cybersecurity Is an Ongoing Journey*
- *New systems, services, apps, software*
- *Hackers always want to hack new things*
- *Old things also they want to hack!*
- *Hackers always finding new ways to hack*
- *Hackers community collaborate strongly*
- *Digital Transformation = quick adoption of new IT services*
- *Pandemic lockdown adds to quick adoption of new IT systems & service*



## Cyber Security:

# LAND ADMINISTRATIONS TODAY :

### Fragmented IT

- Old Legacy Core Systems
- Not Integrated Procedures
- Fragmented Infrastructure and Policies
- IT is often a separate department
- Many different vendors and tech
- Very difficult processes to upgrade
- Internet demand on e-services is very high

### CS Culture

- Cyber Security is not part of the culture
- Unless an incident occurs no-one is being proactive enough
- Leaders believe is a technical issue only
- IT management is not embedded in top management
- Data fraud or breaches are very minimal or close to none – lets not worry!

### People / Skills

- Lack of people and skills on CS
- Obstacles in building Incident Response Plans
- Obstacles in understanding the value of business continuity plans
- Technology is a speedy train, LA cannot follow timely

### CS Infrastructure

- Lack of SOC Intelligence
- No pro-activeness
- Digital Security Authorities are new-born
- Lack of horizontal continuity among Governments
- New laws difficult to implement – NIS Directive
- High costs to implement
- Usually not a priority
- Practical problems



## Cyber Security:

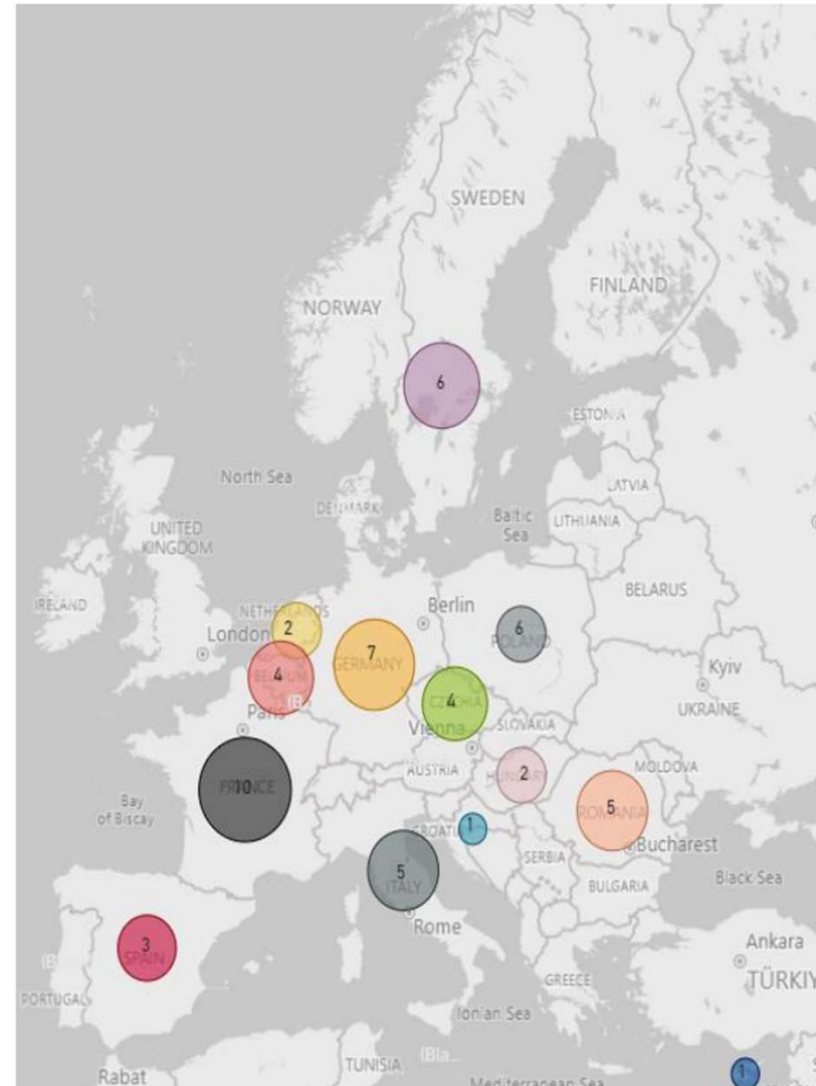
# Important Facts:

The prior reporting period saw cybercriminal, nation-state and hacktivist activity continue to impact entities across Europe and the wider world.

Ransomware groups were particularly active, with major entities targeted such as the global fintech firm EquiLend and the Croatian Financial Services Supervisory Agency, as well as Schneider Electric's Sustainability Business division. Several water and wastewater services entities were also impacted during the reporting period, including the UK's Southern Water and Veolia North America -- both private utilities reportedly targeted by ransomware operators.

Microsoft also released an update concerning APT29's breach of its corporate email accounts, stating that further compromises of other Microsoft 365 customers have since been detected. Meanwhile, ESET published research on efforts by the China-nexus Blackwood APT to deliver spyware to manufacturing, trading, and engineering companies via legitimate software updates, while the North Korean ScarCruft APT was observed targeting cybersecurity researchers with the RokRAT backdoor.

Hacktivist activity related to the war between Israel and Hamas remained consistent with prior reporting periods, with Anonymous Arabia and Anonymous Sudan targeting the Israeli telcos CellCom and Pelephone Communications whilst Toxcar Cyber Team claimed to have exfiltrated data from the Mossad and IDF. Concerning hacktivist activity connected to the war between Russia and Ukraine, several Ukrainian state-owned organisations were reportedly disrupted during the reporting period, including energy, transport and postal service entities. These attacks come following claims by Ukraine's GUR regarding destructive attacks conducted against the Russian IT and defense contractor IPL Consulting, as well as other self-attributed disruptive cyber-attacks targeting Russian entities claimed by pro-Ukrainian groups.











# Cyber Security:

## Important Facts:

<p><b>RANSOMWARE</b></p>		<p>Trend →</p>	<p><b>DOS/DDOS</b></p>		<p>Trend →</p>
<p>During this reporting period, ransomware attacks continued being the most popular threat type, with events recorded in BE, FR, PL, DE, CZ, IT. Manufacturing, banking, healthcare and the food sector had been among the victims.</p>			<p>DDoS attacks persisted at a steady level, remaining the preferred threat vector by the hacktivist groups. Most affected EU countries have been RO, PL, BE, FR and DE.</p>		
<p><b>DATA BREACH</b></p>		<p>Trend →</p>	<p><b>DESTRUCTION</b></p>		<p>Trend →</p>
<p>The current week saw an uptick in data breach incidents in contrast to the prior week; nevertheless, the majority were minor in nature with limited impact. One noteworthy exception has been the massive data leakage of a collection of past data leaks totalling over 26 billion records.</p>			<p>Throughout the past week, our records show a lack of prominent destructive cyber events within the European Union.</p>		

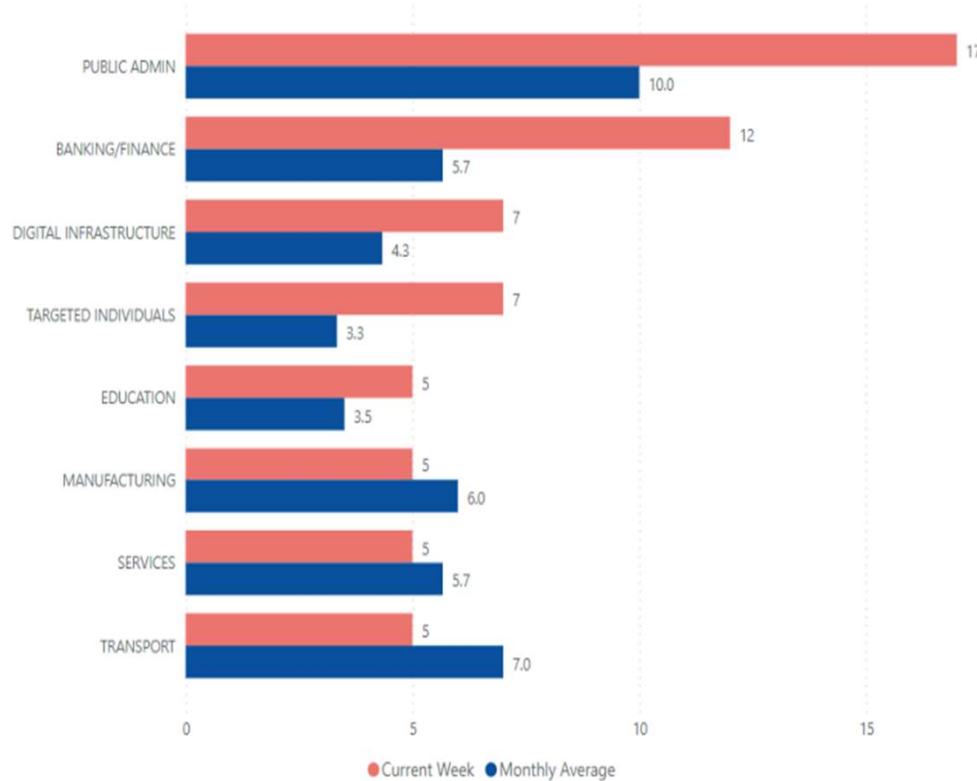


# Cyber Security:

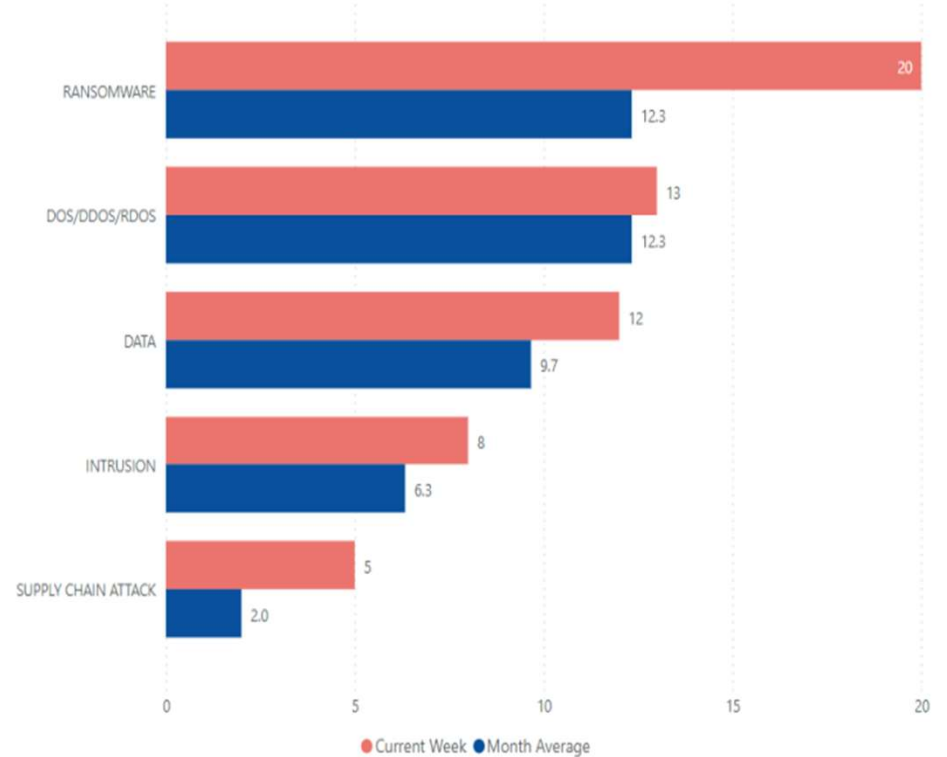
## Important Facts:

### THREAT TYPE AND SECTORS<sup>23</sup>

Incidents per Sector



Incidents per Threat Type







# 8<sup>TH</sup> MARCH 2023

# THE INCIDENT









```
#define MAX_ELEMENT_SIZE 32768
struct QElement
{
    int nSequence;
    int nRecvOffset;
    char m_Buffer[MAX_ELEMENT_SIZE];
};

void jtv_test_streamsummary() {
    std::wstring data;
    if(jtv_api::streamsummary(data, L"", L""))
        std::wcout << data << std::endl;
}

class jtv_api {
private:
    jtv_api() {}
    ~jtv_api() {}
private:
    jtv_api(const jtv_api&);
    jtv_api& operator=(const jtv_api&);
public:
    static bool streamsummary(std::wstring& data,
        const std::wstring& channel,
        const std::wstring& category,
        const std::wstring& language)
    {
        std::wstring rpath = L"/api/stream/summary";
        rpath += L"&mail=";
        // add query part
        std::wstring qry = L"";
        if(!channel.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"channel=";
            qry += channel;
        }
        if(!category.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"category=";
            qry += category;
        }
        if(!language.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"language=";
            qry += language;
        }
        if(!qry.empty()) {
            rpath += qry;
        }
    }
};

#define MAX_ELEMENT_SIZE 32768
struct QElement
{
    int nSequence;
    int nRecvOffset;
    char m_Buffer[MAX_ELEMENT_SIZE];
};

void jtv_test_streamsummary() {
    std::wstring data;
    if(jtv_api::streamsummary(data, L"", L""))
        std::wcout << data << std::endl;
}

class jtv_api {
private:
    jtv_api() {}
    ~jtv_api() {}
private:
    jtv_api(const jtv_api&);
    jtv_api& operator=(const jtv_api&);
public:
    static bool streamsummary(std::wstring& data,
        const std::wstring& channel,
        const std::wstring& category,
        const std::wstring& language)
    {
        std::wstring rpath = L"/api/stream/summary";
        rpath += L"&mail=";
        // add query part
        std::wstring qry = L"";
        if(!channel.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"channel=";
            qry += channel;
        }
        if(!category.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"category=";
            qry += category;
        }
        if(!language.empty()) {
            if(!qry.empty()) {
                qry += L"&";
            }
            qry += L"language=";
            qry += language;
        }
        if(!qry.empty()) {
            rpath += qry;
        }
    }
};

// Skin Window Message Procedure
def SkinWndProc(str):
    operator = string.split(str.value, "&")
    ## pressed off
    if operator[0] == "btn_close":
        HelloWorld.SendSkinMessage("wndmgr", "cls", "hello")
        HelloWorld.FinalSkin()
        EndPumpMessage()
    pass

HelloWorld = CBrandNewUI(" \\BrandNewUI.dll", "\\HelloWorld\\HelloWorld.xml")
HelloWorld.LoadModule()
HelloWorld.InitSkin()
```





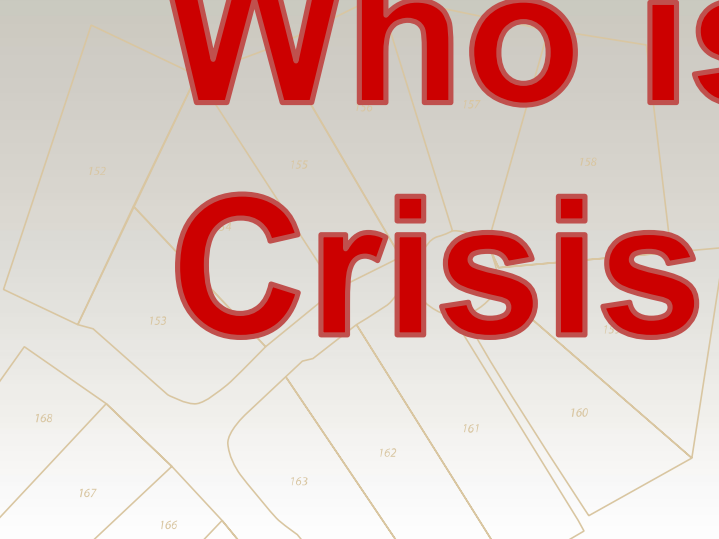


# CYBER ATTACK

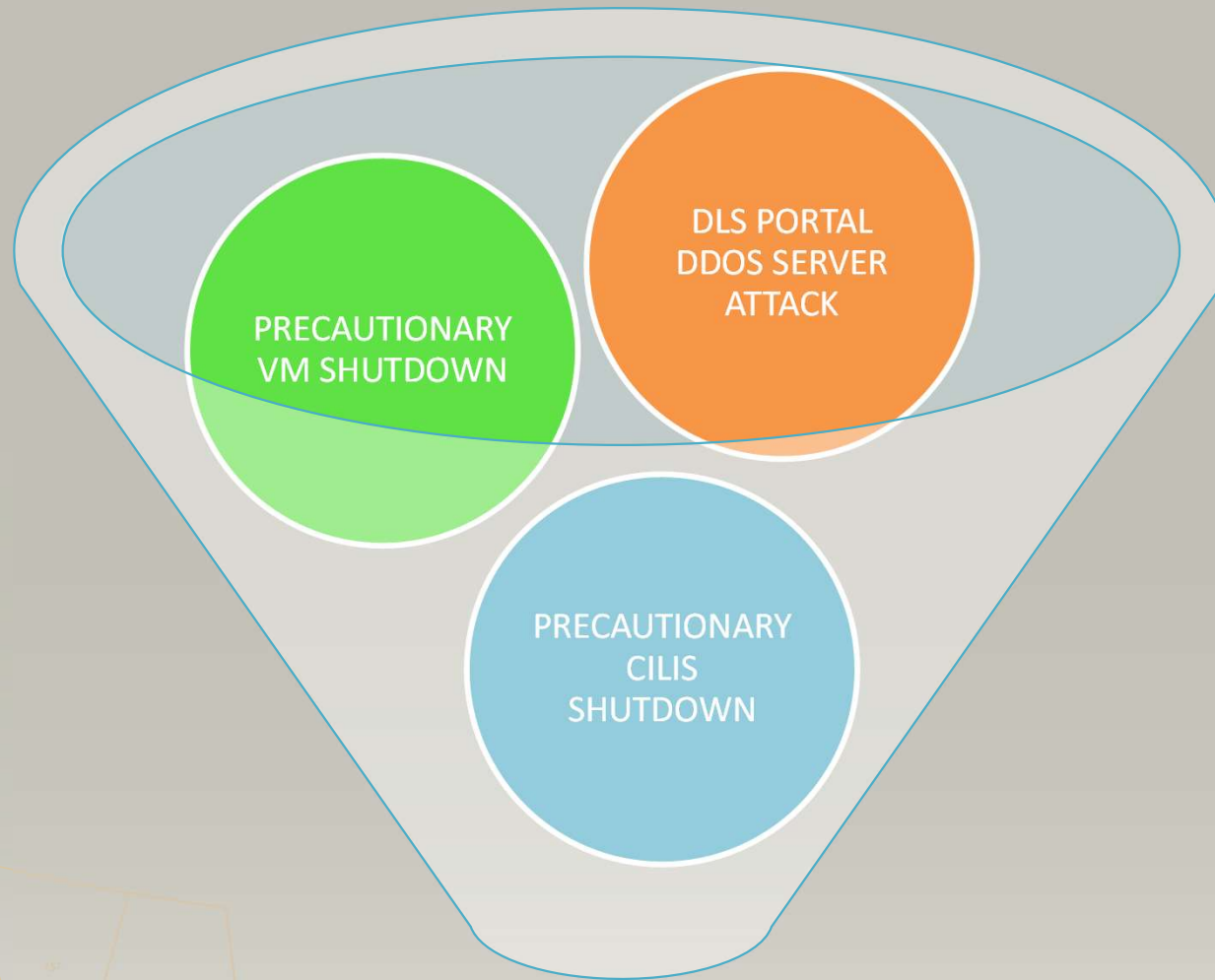
Where is the Plan?

Who is the Leader?

Crisis Management

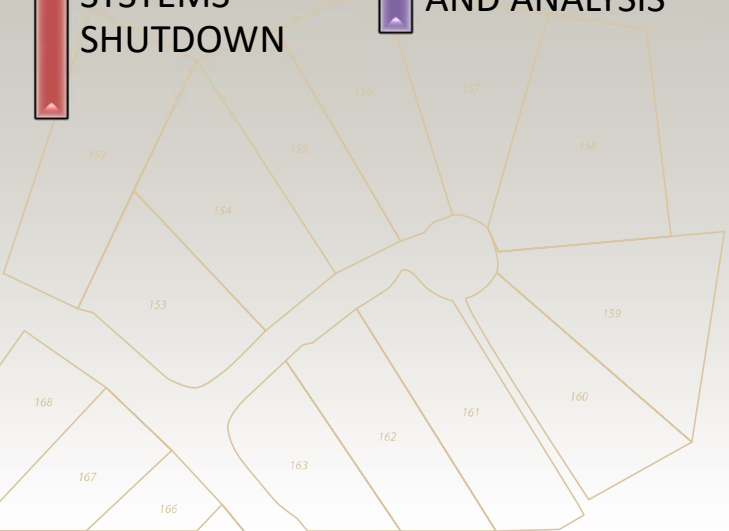
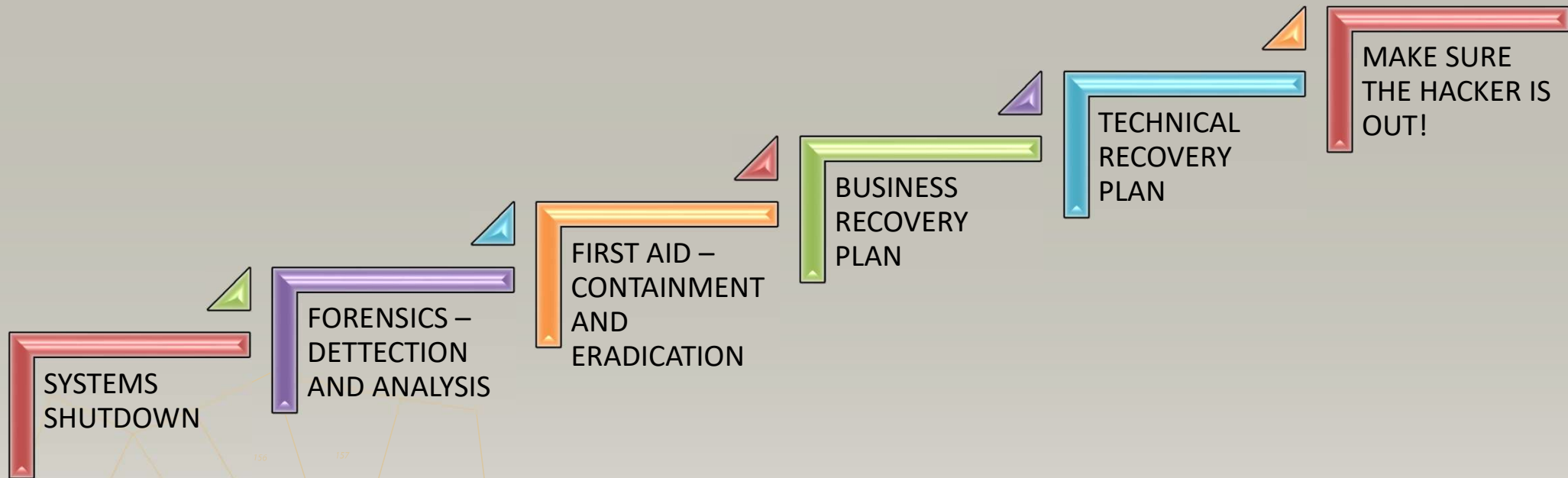






**CYBER ATTACK INCIDENT OFFICIAL  
RESPONSE PROTOCOL INITIATED**







# CYBER ATTACK

## Million \$ Question!











LESSONS LEARNED #1!

NO No. 2# !!

100 Decisions to be taken – Need to be 100% Correct !!

Disaster Management – From theory to practise!

Many Stakeholders Involved – Who is the Boss (Project Manager)?!

Many Vendors Involved – Many Procedures to align

Need strong procedures – Effective Leadership



# MOST CRITICAL ASPECT COMMUNICATION!





COMMUNICATION STRATEGY – HUMAN RATHER THAN TECH

CONVINCE THAT THERE WERE NO DATA BREACHES

THE PUBLIC – THE ECONOMY IMPACT (SEVERE COSTS)

1000 EMPLOYEES – 800 MACHINES – LARGE IT INFRASTRUCTURE

FIRST TIME EXPERIENCE

INCREMENTAL RECOVERY VS FORENSICS

DO YOU HAVE A PLAN B – A PLAN C?! – BUSINESS CONTINUITY

## Lessons Learned – The DLS Case:

### Our Experience:

**PLANS – FROM THEORY TO PRACTISE**

**MOST DECISIONS ARE NOT TECHNICAL**

**TECHNICAL SOLUTIONS: STANDARD**

**MOST CRITICAL DECISIONS: BUSINESS**

**HACKERS DID NOT AIM DATA**

**WANTED TO HALT OPERATIONS**

**OUR IMAGE**

**DID NOT SUCCEED THE 1<sup>ST</sup> TIME**

**2 ADMINISTRATIVE PROCEDURES**

**LEGAL CONSEQUENCES / PENALTIES**

## Lessons Learned – The DLS Case:

### The result:

**DLS WAS PREPARED**

**PROCEDURES IN PLACE FOR AN INCIDENT**

**NEEDS IMPROVEMENT – FORMA WAY**

**FIRST AID CAME QUICK**

**HALTING OPERATIONS WAS CRITICAL**

**INCREMENTAL – 1<sup>ST</sup> OFFICE IN 7 DAYS**

**REBUILT DLS PORTAL FROM DR**

**ELEVATED THE LEVEL OF SECURITY**

**BARACCUDA FIREWALS – PEOPLE COMPLAIN**

**NEED TO STRIKE A BALANCE**

**SECURITY VS CUSTOMER SERVICE**





# CYBER SECURITY

**Our Advice:**

**We all are**

**Critical Infrastructure**

**BE PROACTIVE**



# CYBER RESILIENCE



# CYBER RESILIENCE

INCIDENT  
RESPONSE  
PLAN

DISASTER  
RECOVERY  
PLAN

BUSINESS  
CONTINUITY  
PLAN



## Cyber Resilience:

# The way forward:

**False  
Sense of  
Security**

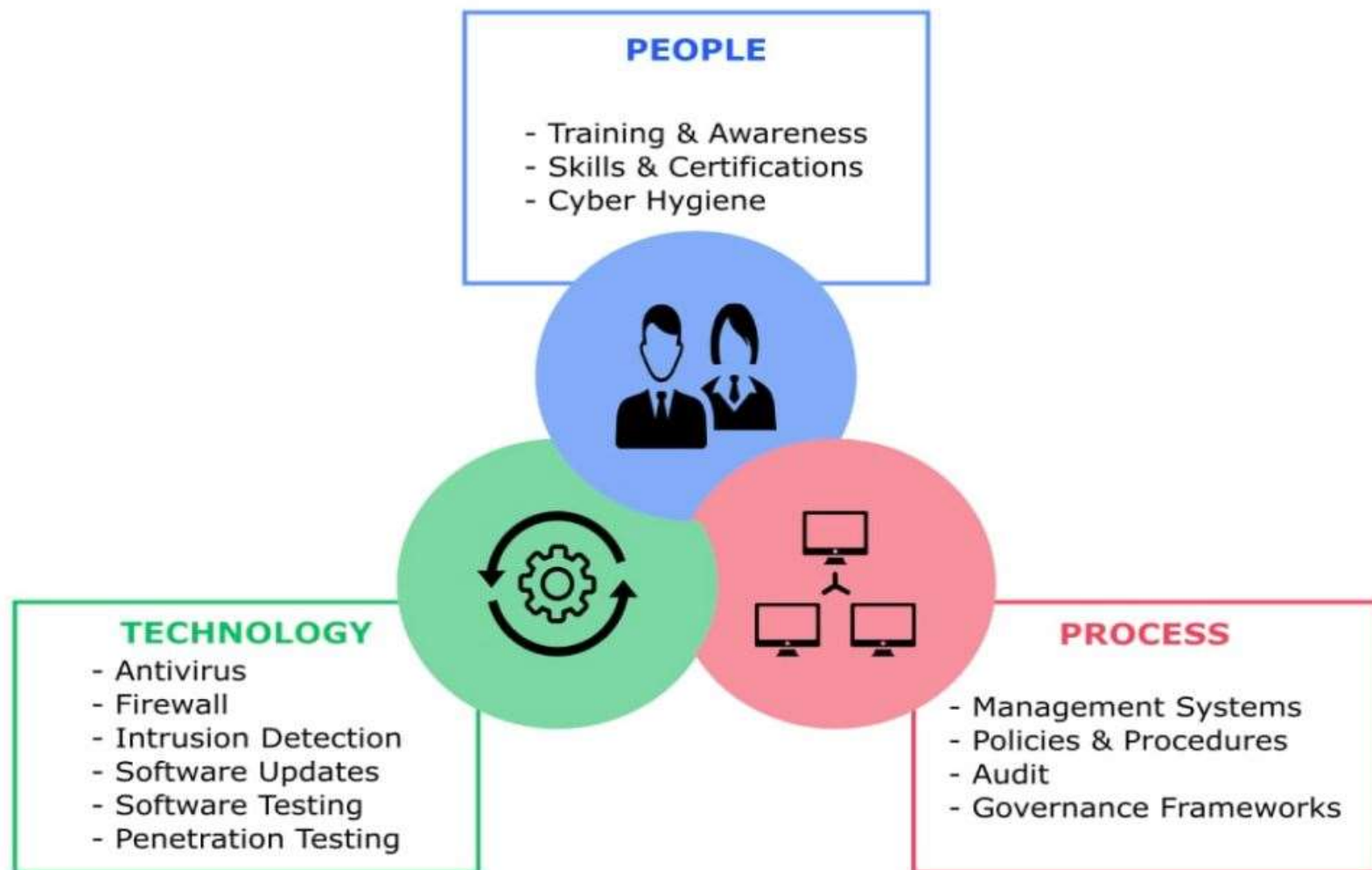
**People and  
Processes**





# Cyber Resilience:

## Three Pillars of Cybersecurity: The Foundation of Effective Cybersecurity



# Cyber Resilience – Various Models to Use:





## Cyber Resilience – Various Models to Use:

### CIA Model:

- **ISO 27001 Standard**
- **GDPR Article 32**
- **Confidentiality:** *protecting information such that only those with authorized access will have it*
- **Integrity:** *the veracity and reliability of data. Data must be authentic, and any attempts to alter it must be detectable*
- **Availability:** *data is only useful if it is accessible. Availability ensures that data can be accessed when needed and will continue to function when required.*



# THE ROAD FORWARD CYBER SECURITY STRATEGY







# THE ROAD FORWARD FOR LAND ADMINISTRATIONS **DEVELOP YOUR BUSINESS CONTINUITY PLAN**





Allow for improved cybersecurity measures, including better data protection, intrusion detection, and rapid incident response

Address complexities related to systems and data interoperability and provide solutions.

Ensure that DLS can leverage the latest technology and tools for communication, data backup, and disaster recovery

Address data storage, backup, and recovery to ensure continuity in government operations, especially in situations where data loss could be catastrophic.

Allow DLS to adapt to new types of threats and challenges

Optimize resource allocation, ensuring that essential services can continue with minimal disruption while non-essential functions are temporarily reduced or suspended

Ensure that critical information reaches the public, employees, and stakeholders during a crisis



# THE ROAD FORWARD IN CASE YOU DO NOT DEVELOP YOUR BCP





Ineffective Response to Crisis

Service Disruption

Data Loss

Cybersecurity Vulnerabilities

Loss of Public Trust

Legal and Regulatory Non-Compliance

Inefficient Resource Allocation

Economic Impact

Reduced Resilience





# THE ROAD FORWARD CRITICAL MILESTONES





EMBED CS IN CO CULTURE

Risk Assessment

IT Governance

Training and Awareness

Data Management Processes

System Security

Patch Management

Data Availability in Crisis



BCP

Disaster Recovery Plan

Incident Response Plan

Continuous SOC Operations

Vendor Relations and Continuity Plan

Business Impact Analysis

Current / Future Architecture Limitations

Physical Security

Testing and Updating of Plan

**GOOD LUCK ! It all comes down to people!**



**Working Party on  
Land Administration**



DEPARTMENT OF LANDS AND SURVEYS - CYPRUS

**How are land administrations responding to evolving threats to maintain system security?**

**The recent case of the DLS – Cyprus**

---

**NEOCLIS NEOCLEOUS – CHIEF LANDS OFFICER**

*UNECE WPLA WEBINAR – CYBER SECURITY*

*22<sup>ND</sup> FEBRUARY 2024*