



# Cybersecurity Consulting Services *A necessity?*

**Logicom**  
Solutions

**Nikos Tsalis, PhD**

**Head, Information Security,  
Business Consulting Services**



# This is what has been predicted for 2019 for cybersecurity



Nations At Cyberwar

Supply-Chain Attacks  
Rise

Cybersecurity Raises  
Its Profile In The  
Boardroom

Enterprise Approach  
To Cybersecurity



# And this is what happened in only in one month's time

Cyber attacks

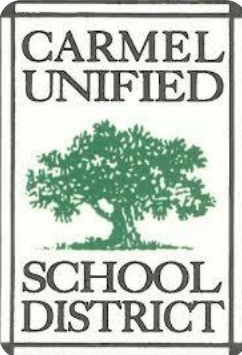
Data breaches

Ransomware

Financial information





**2.1 billion** records leaked



# Impact on the organization

**Reputation Lost**



**Limited Customer trust**



**Decreased Competitive ability**



**Reduced Revenue**



**Fines**



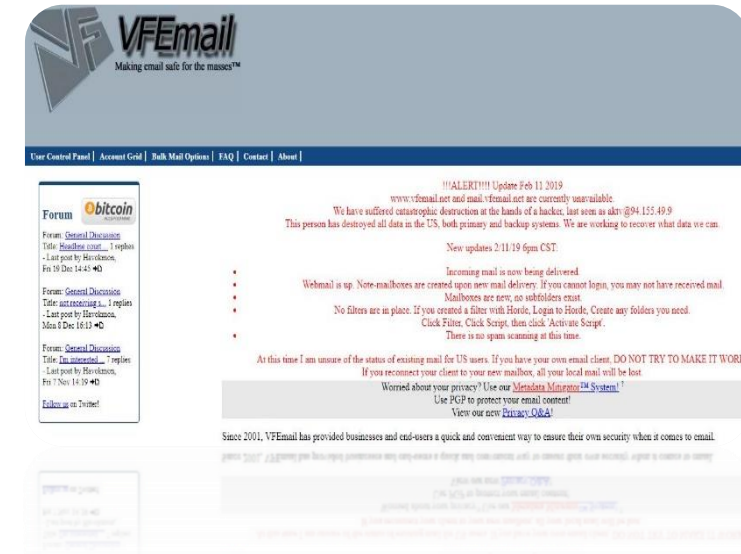
# Some real life recent examples...

**TIMES MALTA**

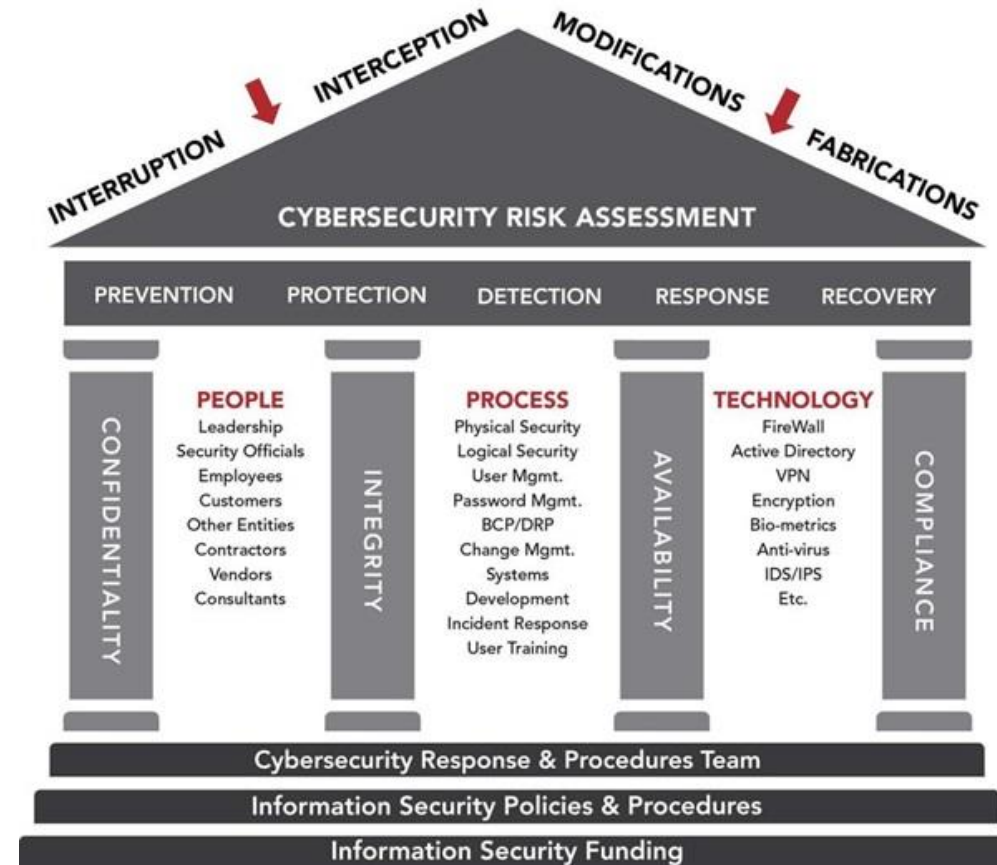
Thursday, February 14, 2019, 07:55

## Bank of Valletta resumes operations after major cyber attack

Payments to third parties not yet activated



# A need for a holistic approach





# Business case: The good, the bad and the ugly 😊

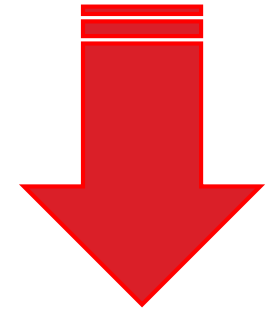
Holistic cybersecurity  
framework



The correct way to do it



The wrong way to do it



Fragmented cybersecurity  
framework

# Cybersecurity best practices



## Solid framework

It is important to have a clear scope of the cyber security scope, within the organization, and how to manage it appropriately.



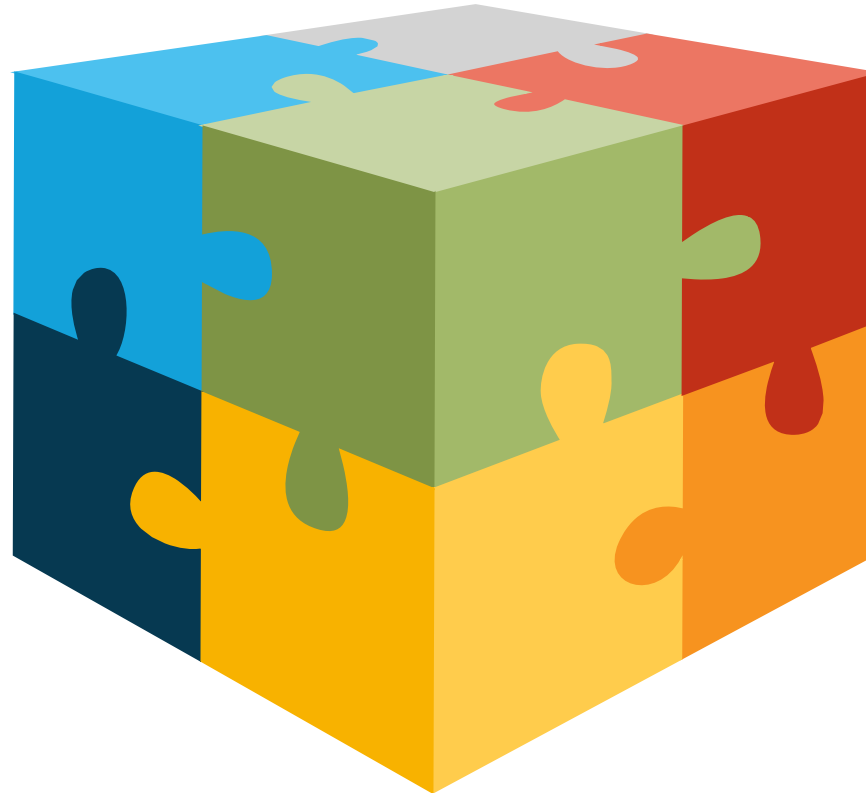
## Leadership

The cybersecurity element must be driven and managed by the organization's management (e.g. Board of Directors), to emphasize on its importance.



## Risk management

Each organization faces specific risks and threats towards its daily operations. All of this elements must be properly identified and coped with, so as to reach an adequate security level.



## Support

The human factor is vital to implement, operate and review the related security controls. Thus, there should be appropriate training and expertise within the organization.



## Security controls

The core of the security framework is the implementation of the appropriate controls, that will strengthen the organization's security posture.

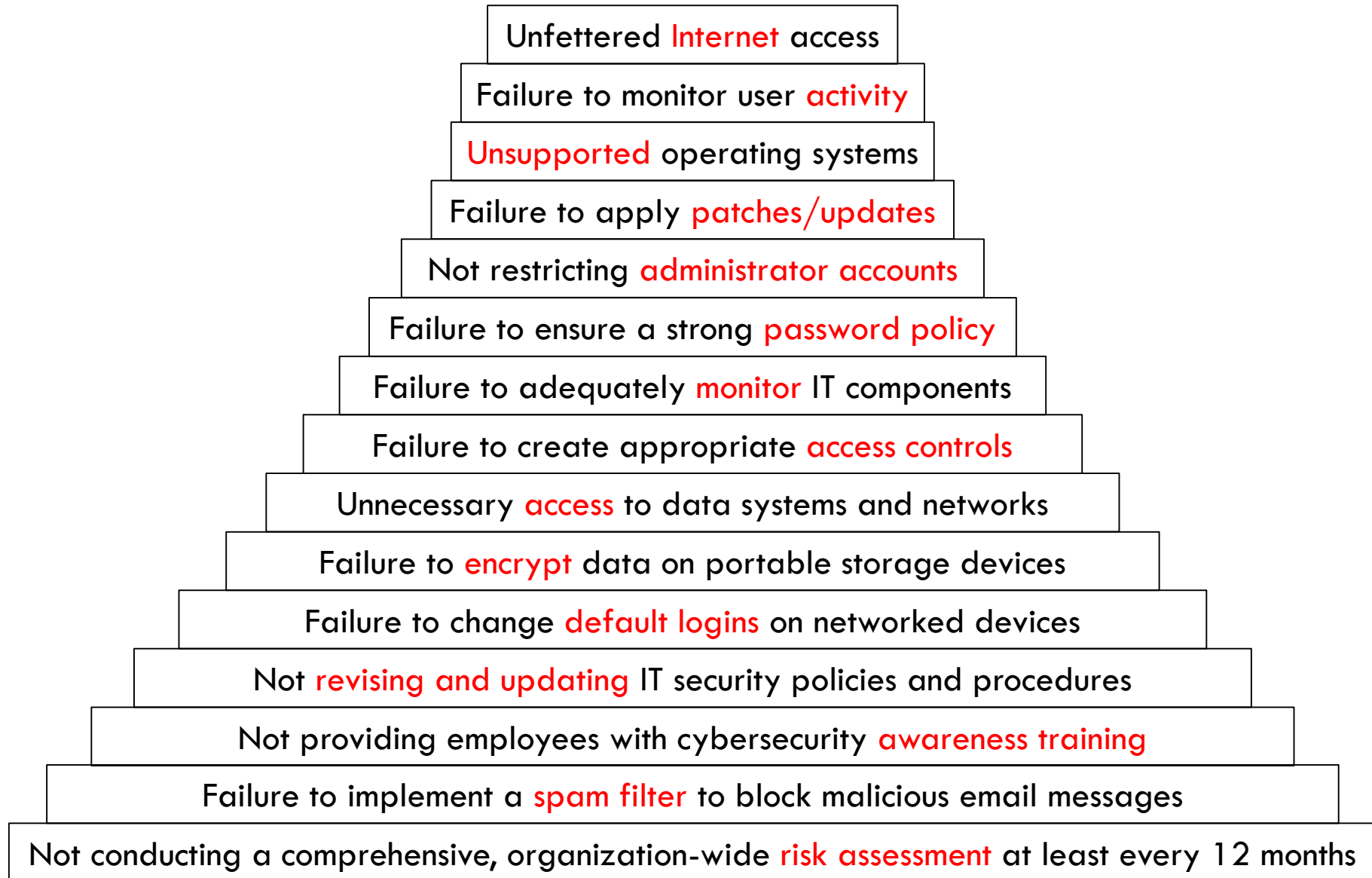


## Improvement

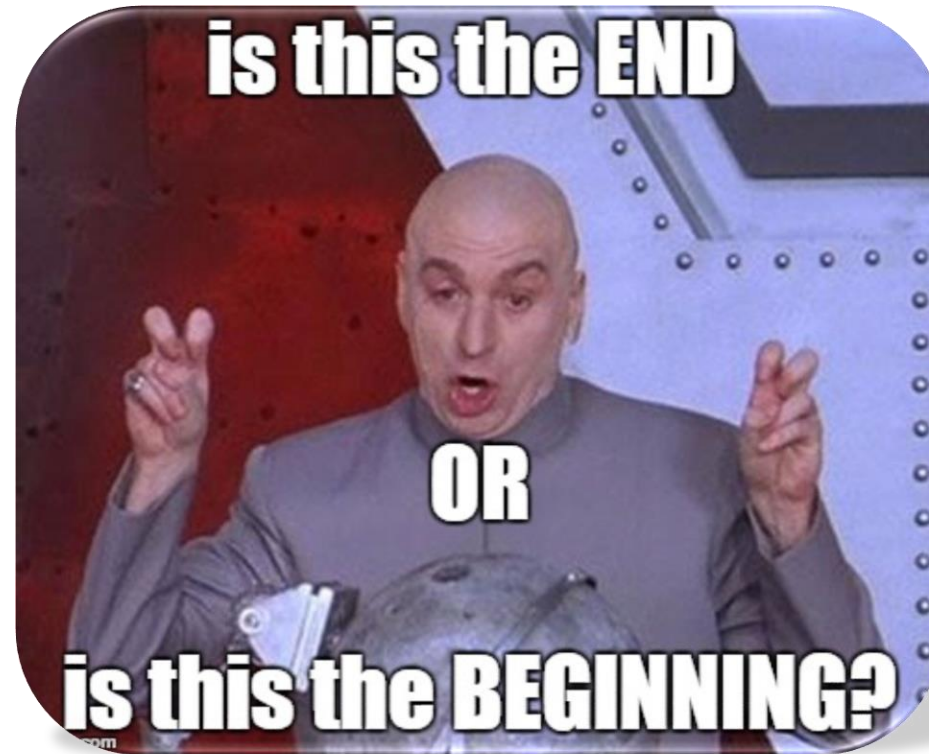
After the successful implementation of the framework, it is important to continuously review and improve all the related components.



# Poor cybersecurity best practices

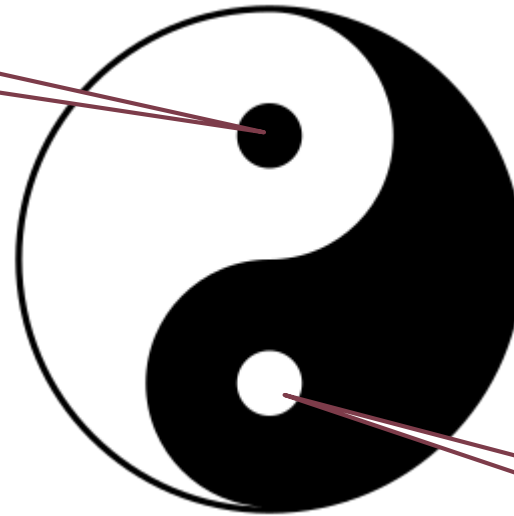


# End of the story?



# We forgot something...

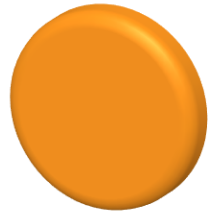
The **Bad** in the **Good**



The **Good** in the **Bad**

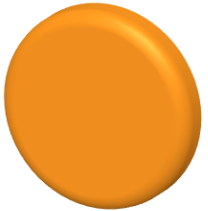


# The **Bad** in the **Good**:



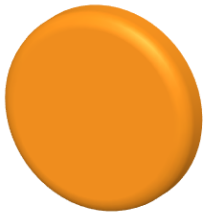
## **LEADERSHIP SUPPORT**

The required guidance from the organization's management must be uninterrupted, to ensure support by all departments.



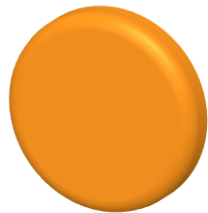
## **CONTINUOUS IMPROVEMENT**

A process to review and re-assess the existing cybersecurity approach is vital to enable a continuous improvement.



## **WEAK IMPLEMENTATION**

It is common to fail to implement the identified control mechanisms (procedures and controls) properly.



## **POOR RISK MANAGEMENT**

Lack of a comprehensive and organization-wide risk management process.



# The Good in the Bad

## INTERNAL EXPERTISE

The specialized employee may be efficient, but he is a single point of failure if he leaves.

## “STRONG” MONITORING

A threat is revealed either via monitoring (detection) or its direct impact within the organization.

## “LOOSE” REGULATIONS

There is a possibility that the organization operates under a loose regulatory framework, and thus, does not have clear security obligations (e.g. bank vs. retail).



## AD-HOC APPROACH

It is common to operate under weak or an ad-hoc security policy framework.

## LUCK

There is often the chance that an organization did not utilize any security controls, because there were no related incidents.

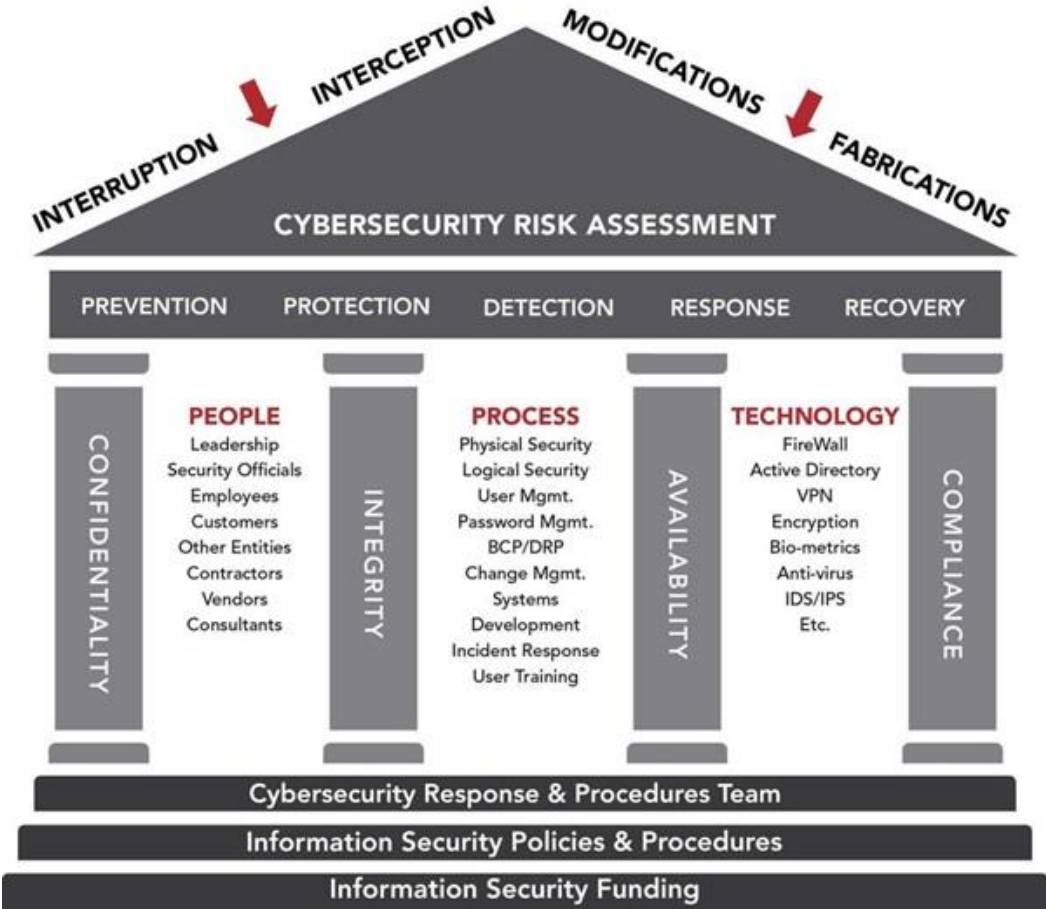
# What's next?





# And the winning answer is...

Holistic approach



Proportionality rule applies here

# The need to support cybersecurity

## CURRENT STATUS

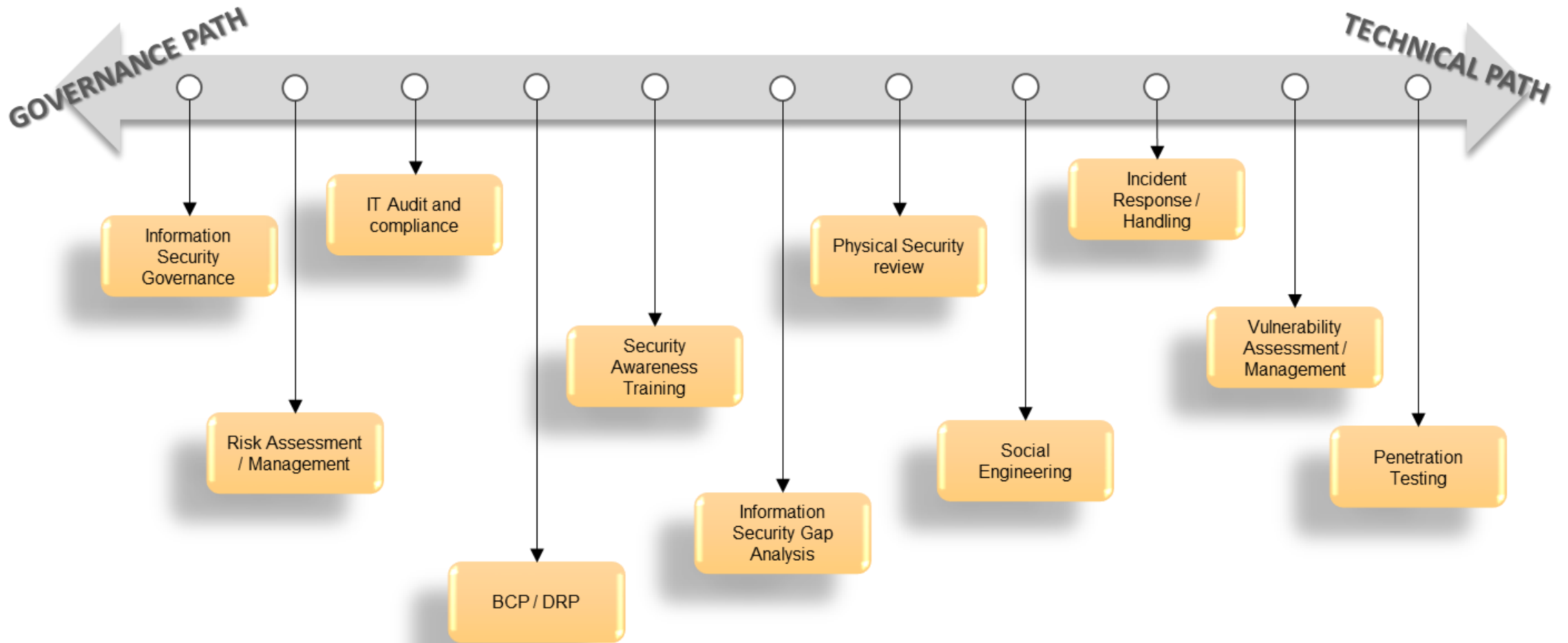
- Understaffed departments
- Lack of expertise/ competences
- Existing operational workload
- Limited budget allocated



## FUTURE STRATEGY

- ✓ Hire additional resources
- ✓ Invest more in cybersecurity
- ✓ Outsource services to third parties

# LGS Cybersecurity Consulting Services





# A FULLY QUALIFIED TEAM



## INDICATIVE PROJECTS IN LAST 6 MONTHS

DISASTER RECOVERY POLICY  
BUSINESS CONTINUITY PLAN



ISO27001 ASSESSMENT



INFORMATION SECURITY GAP  
ANALYSIS



PENETRATION TESTING



DPO SERVICES



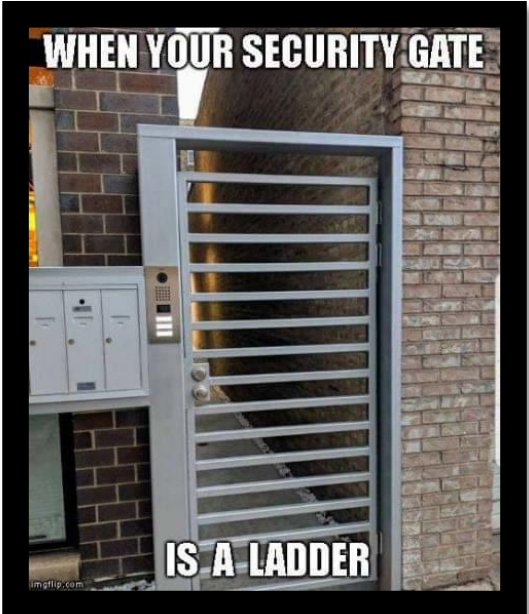
INFORMATION SECURITY  
AWARENESS TRAININGS



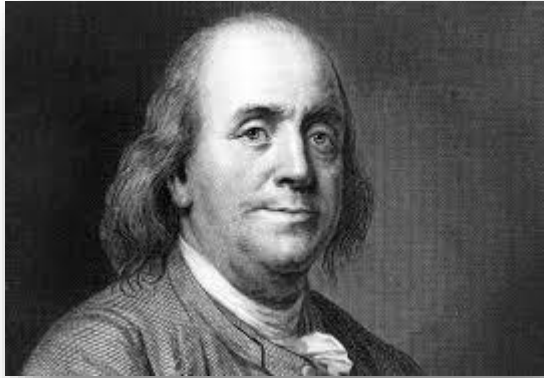
VULNERABILITY ASSESSMENT



# Implementation is also important!



# Always remember



“If you fail to plan, you  
are planning to fail.”

- Benjamin Franklin



Thank  
you!

**Nikos Tsalis, PhD**

**Head, Information Security**

Business Consulting Services

 : [n.tsalis@logicom.net](mailto:n.tsalis@logicom.net)

**Logicom**  
Solutions