



**NORTH TEXAS**  
**ISSA**  
#NTXISSA

# Managing Cyber Security Across the Enterprise

Asif Effendi

September 3, 2015

austinssi >

# Managing Cyber Security Across the Enterprise

## Highlights:



Oil and Gas Threat Landscape



Challenges in Securing Control Systems



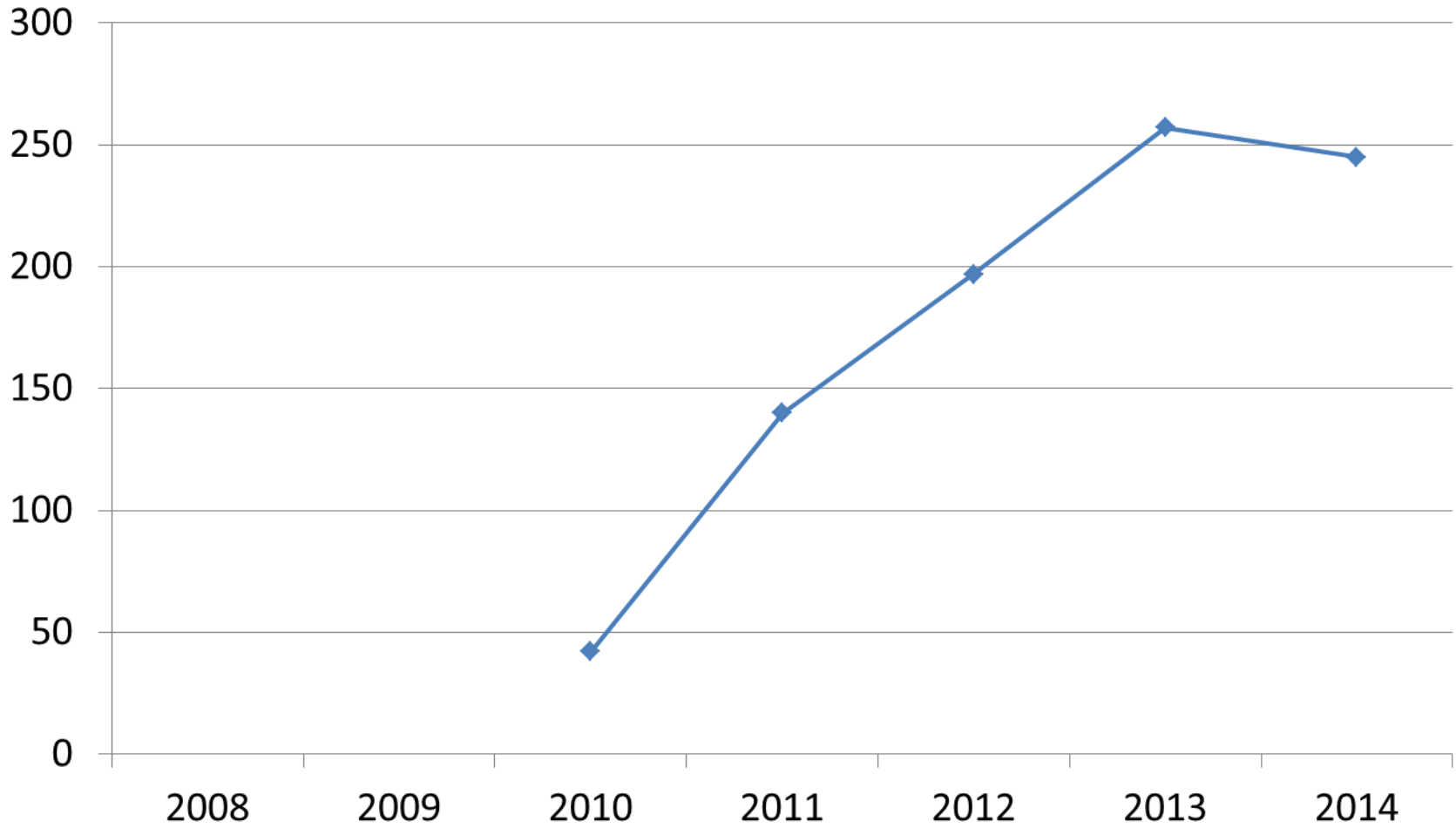
Cyber Security Strategies



Conclusion



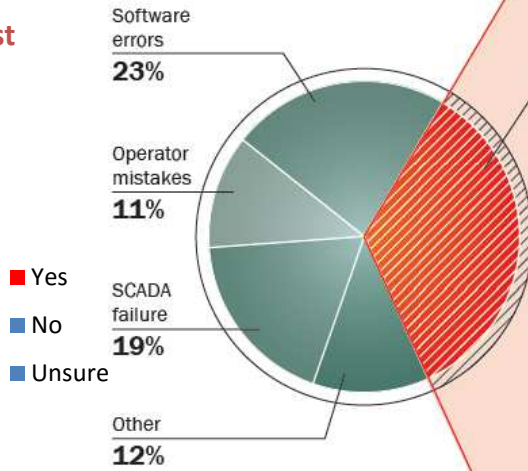
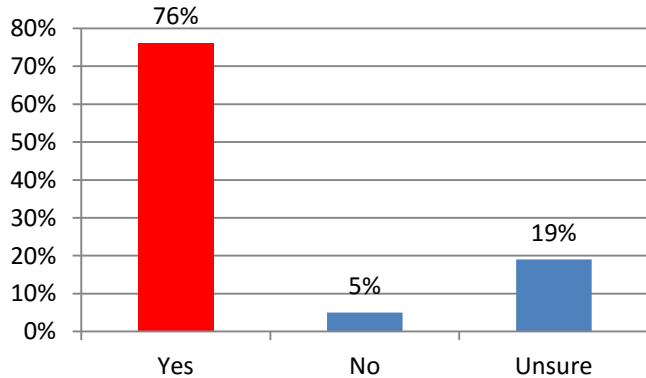
## # of Reported Incidents (ICS-CERT)





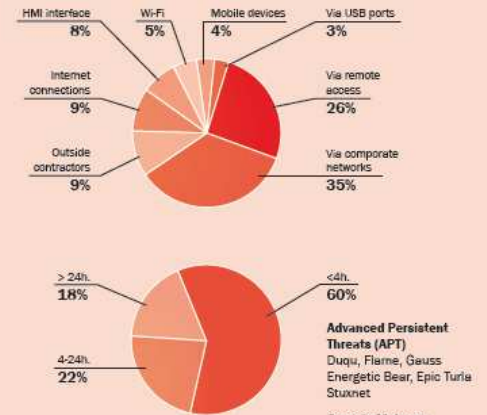
## Increase in sophistication of cyber attacks

### Increase in Sophistication of Attacks Against Infrastructure (2015 Report of Organization of American States)



Major reasons for industrial network malfunction incidents  
**securityincidents.net**

### Malware attacks 35%



**Advanced Persistent Threats (APT)**  
Duqu, Flame, Gauss, Energetic Bear, Epic Turia, Stuxnet

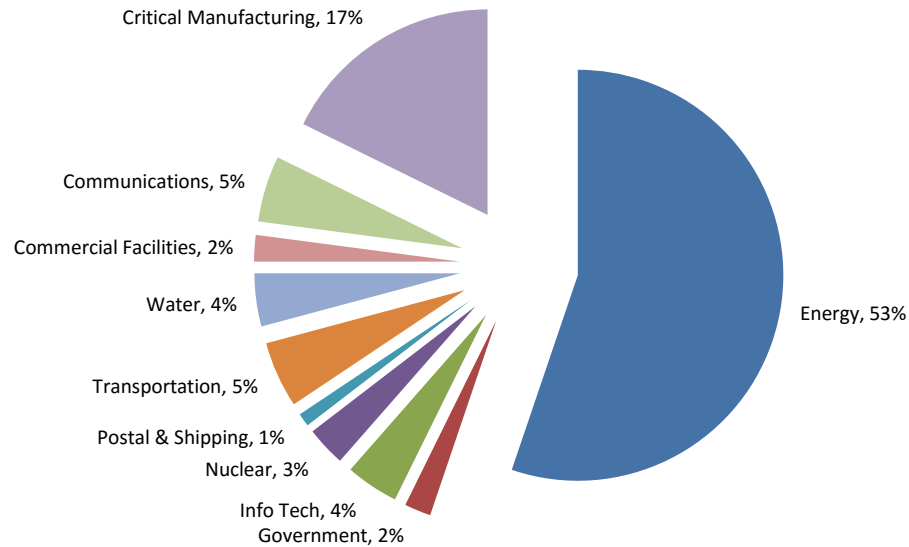
**Generic Malware**  
Many ICS threats are unsophisticated but their impact is massive:  
Worms, Trojans, Blockers, Password theft, remote access, vandalism.

Downtime of the industrial process due to malware incidents  
**securityincidents.net**



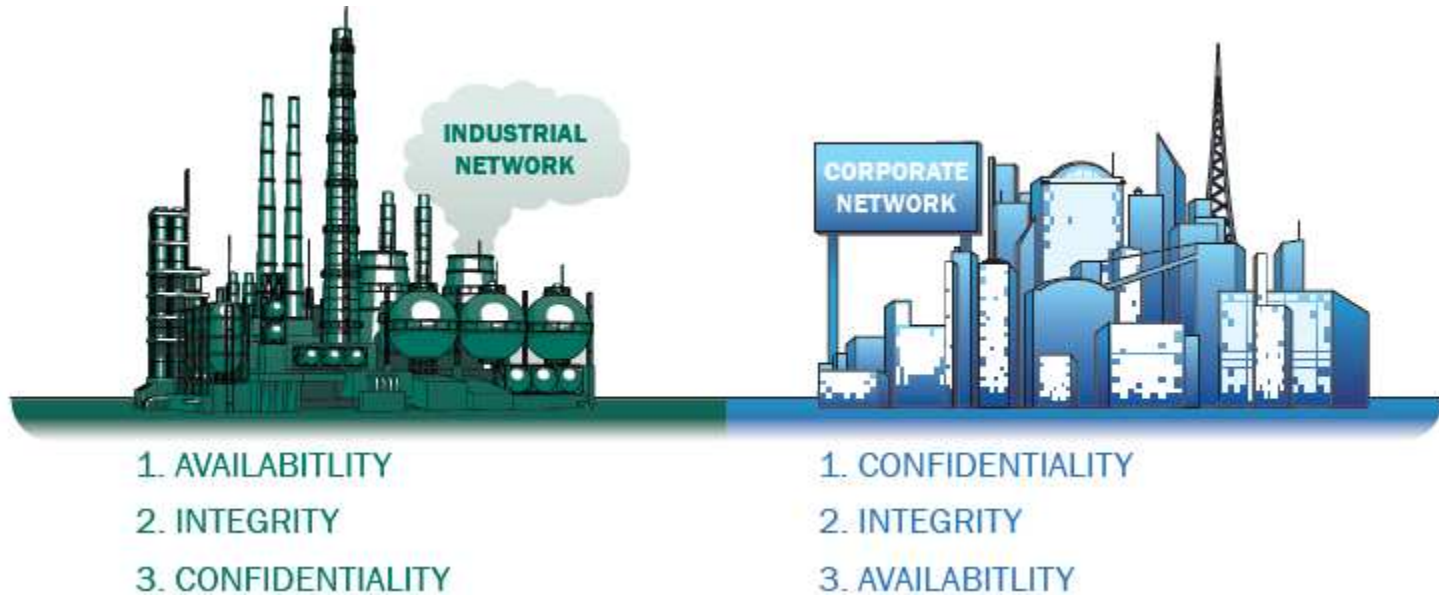
# Largest sector of cyber incidents is Energy industry

Distribution of Cyber Incidents (ICS-CERT)





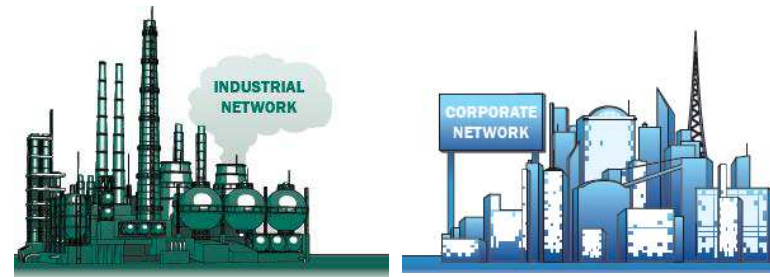
## Difference in security attribute between ICS and Enterprise systems



Courtesy: Kaspersky Lab



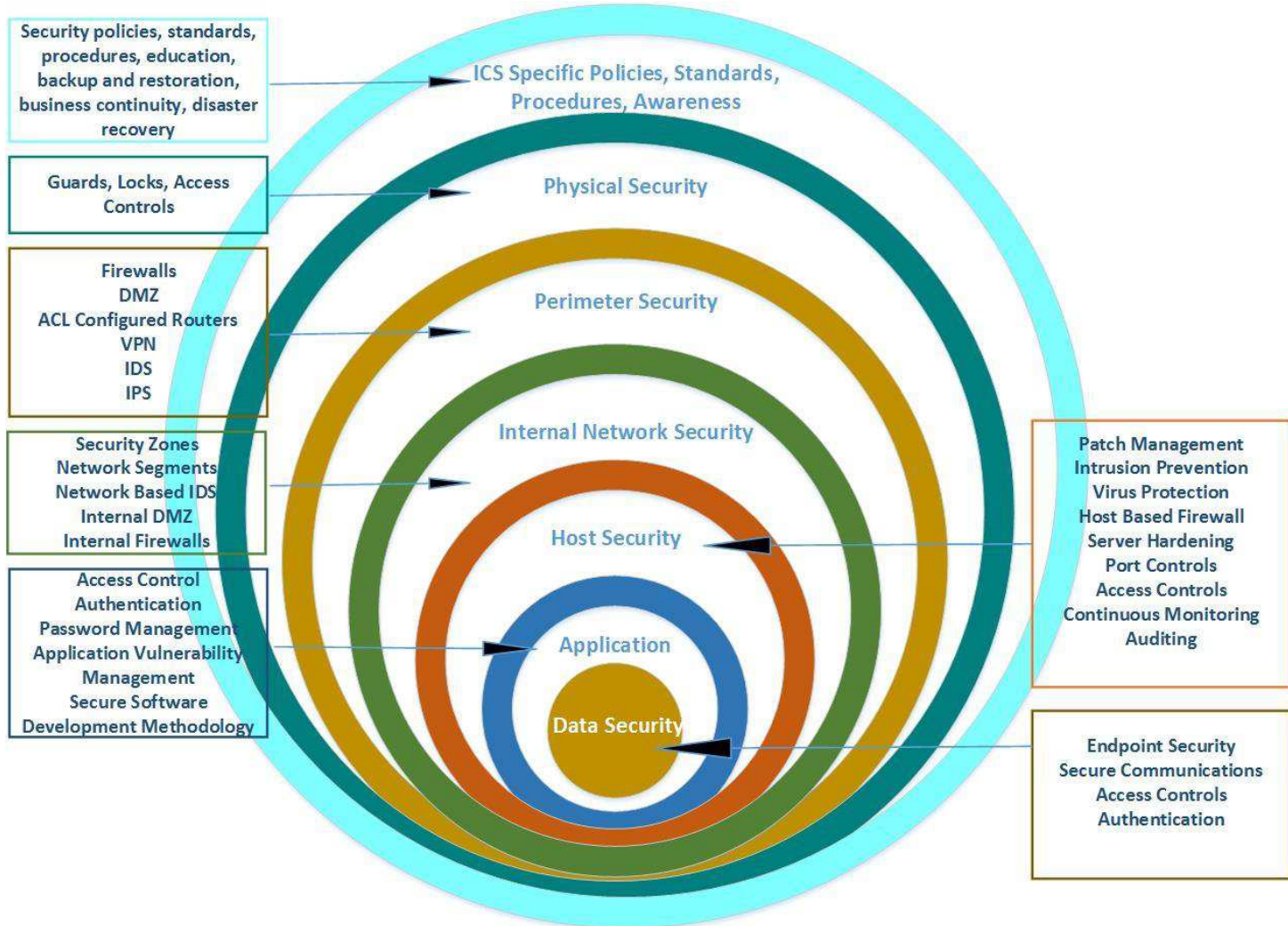
## Differences/similarities in security controls considerations between ICS and Enterprise systems



|   |               |             |
|---|---------------|-------------|
| Life Span                                 | 15 – 20 years | 3 – 5 years |
| COTS Related Vulnerabilities              | Yes           | Yes         |
| Third Party Access to Systems             | Frequent      | Limited     |
| Security Considerations in Implementation | Limited       | Yes         |
| Wireless Access to Systems                | Significant   | Limited     |



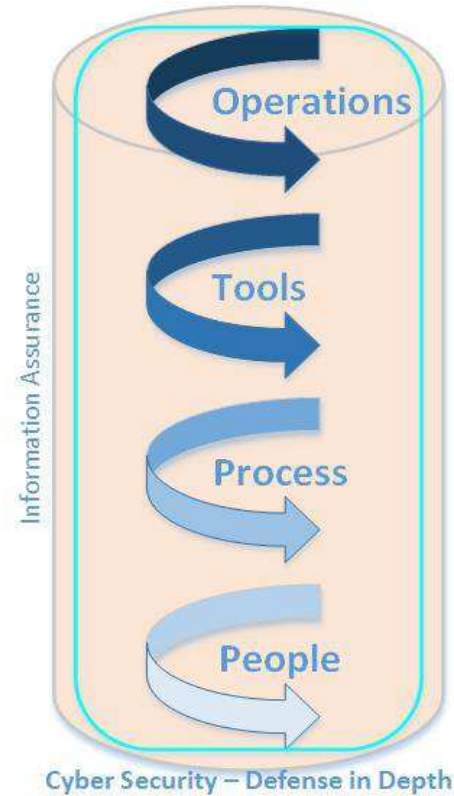
## Defense in Depth in securing ICS





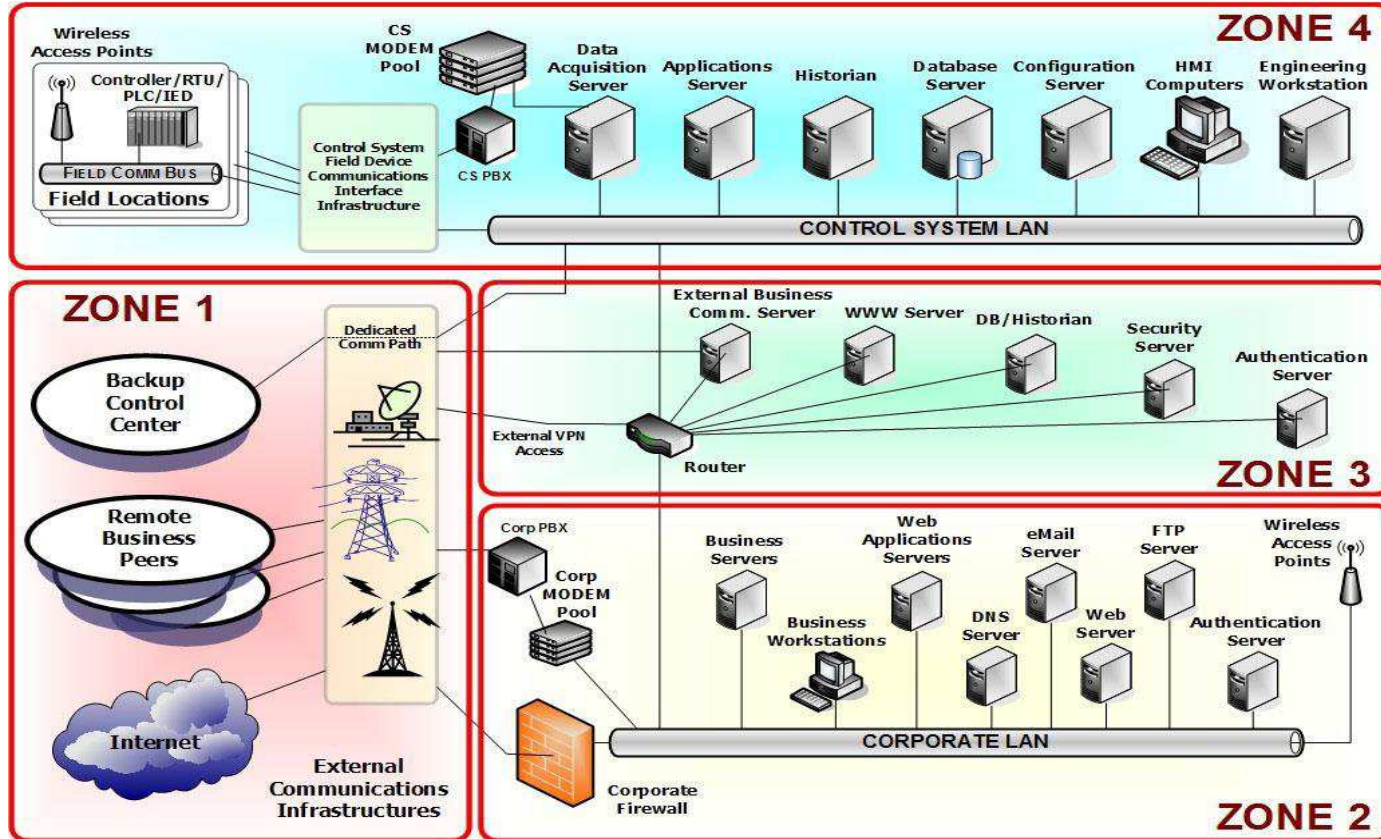


# Risk Based Approach and Management to Securing ICS





## Network Segmentation



(Reference: Defense in Depth Strategies, Idaho National Laboratory, Department of Homeland Security Based on ISA 62443)



## Summary



Rapid integration of “Commercial Off the Shelf (COTS) in ICS environment comes with vulnerabilities and risks



Industrial control systems are not easy to secure



Hacker knowledge base is growing rapidly, resulting in more sophisticated attacks

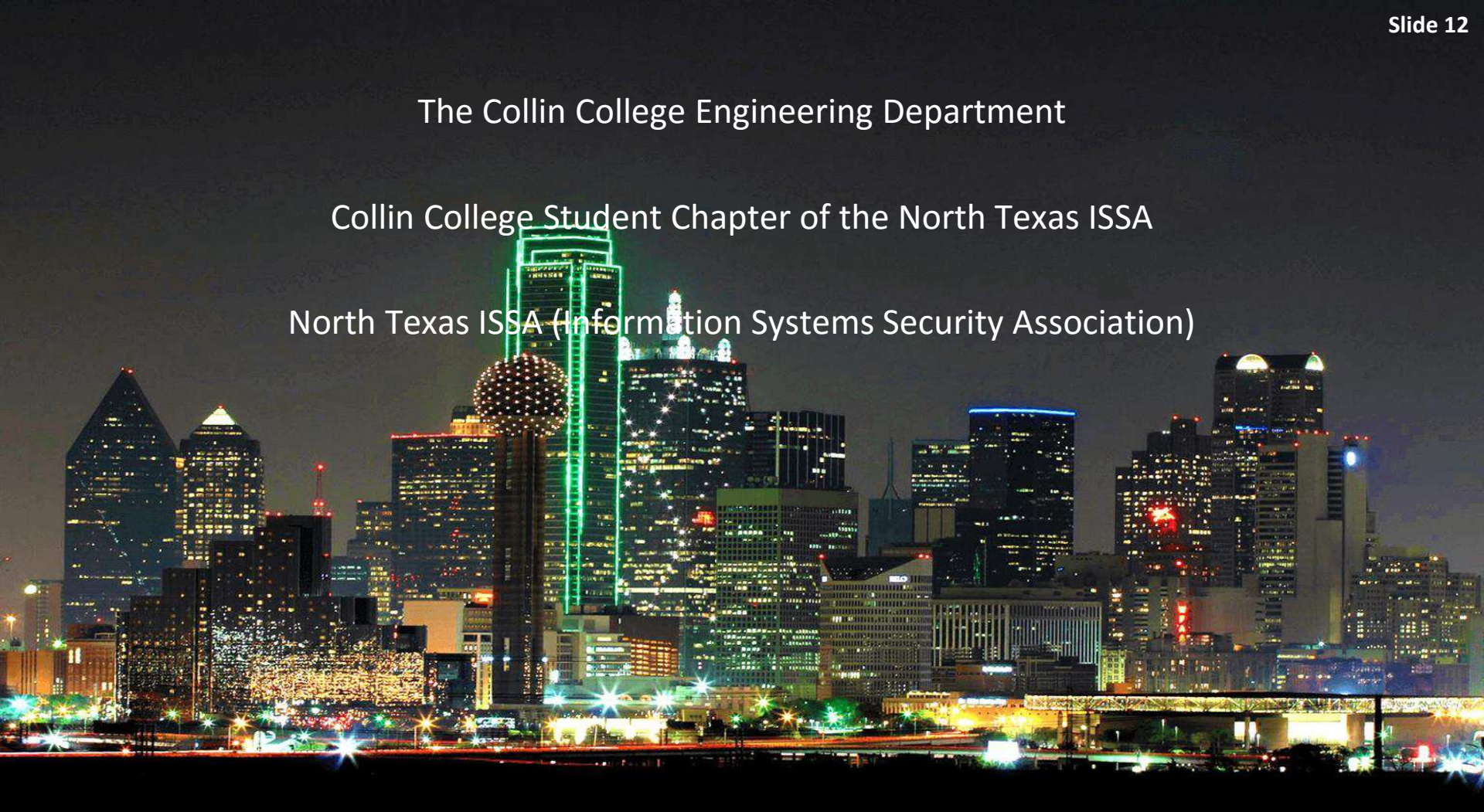


Risk has to be managed although it can not be eliminated. Risk based “Defense in Depth” mitigates cyber risks at multiple layers in an organization

The Collin College Engineering Department

Collin College Student Chapter of the North Texas ISSA

North Texas ISSA (Information Systems Security Association)



Thank you

