Defense in Depth

Constructing Your Walls for Your Enterprise

Mike D'Arezzo
Director of Security
April 21, 2016

SLAIT Consulting

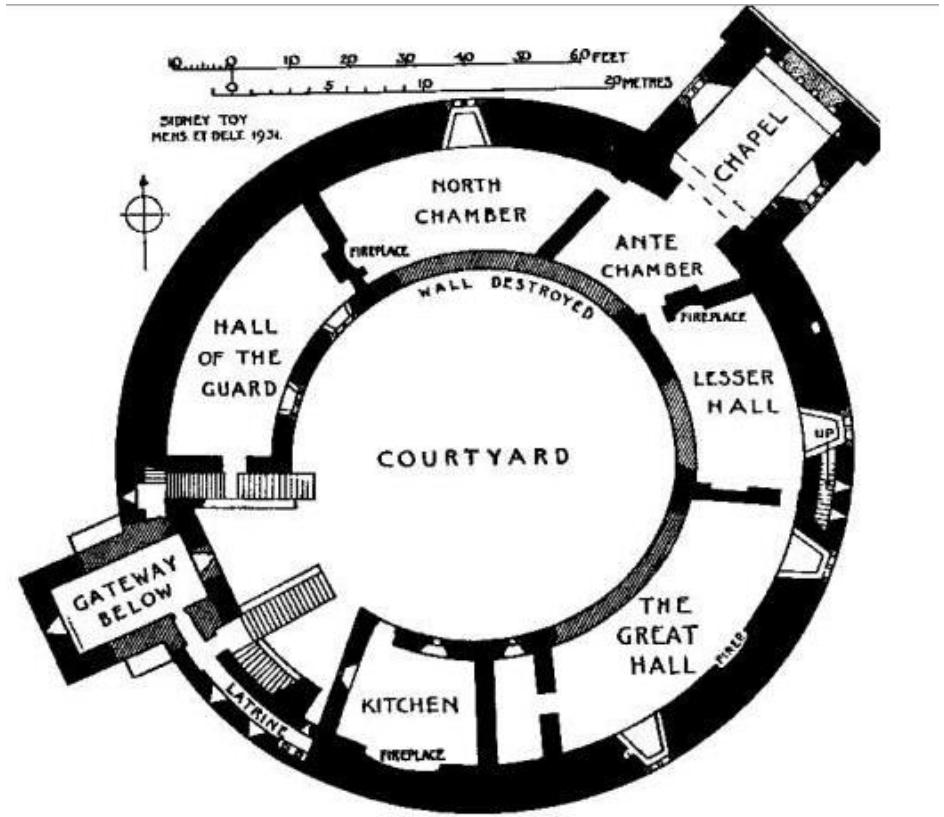
Defense in Depth

Defense in Depth

- Coordinated use of multiple security countermeasures
- Protect the integrity of the information assets
- Based on the military principle that a complex and multi-layered defense is easier to defend a single barrier

SLAIT Consulting

Defense in Depth



Restormel Castle. Plan of Keep, First Floor.

Defense in Depth

- Also known as Castle Approach
- Information assurance (IA) concept in which multiple layers of security controls (**defense**) are placed throughout an information technology (IT) system.

SLAIT Consulting

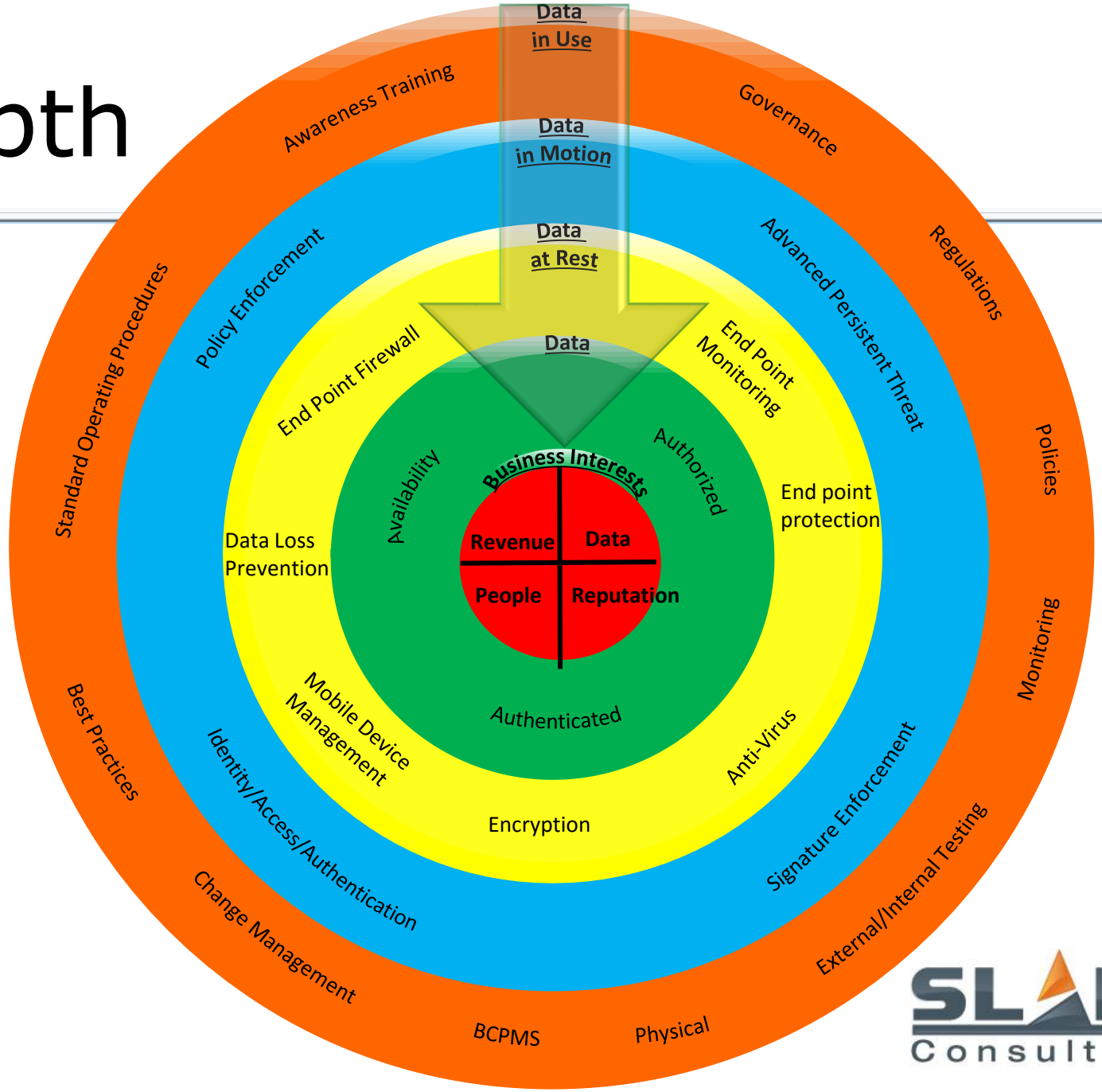
When is enough actually enough?

- Risk Based Approach
  - How much is your data/reputation/revenue actually worth?
  - How much is enough “defense”?
  - When does it become just “noise”?
- Regulatory Compliance
  - What is Required?

SLAIT Consulting

Defense in Depth

- Data
  - People
  - Revenue
  - Reputation
  - Data
- Data in Motion
  - Internal
  - External
- Data at Rest
  - Databases
  - Files and Directories
- Data in Use
  - “People interaction”
  - Processes



SLAIT Consulting

External Threats

- Are you protecting your perimeter?
- Can you verify you are protecting?
- Are you learning as you find threats?
- Are you learning from other's threats?

SLAIT Consulting

Insider Threat

- “Snowden” – does not have to be government secrets
- Would you know if data was lost, copied, or destroyed?
- Sometimes insider threats do not start from the inside….
  - Are you testing phishing campaigns?
  - Are you watching your Highly Privileged Accounts?

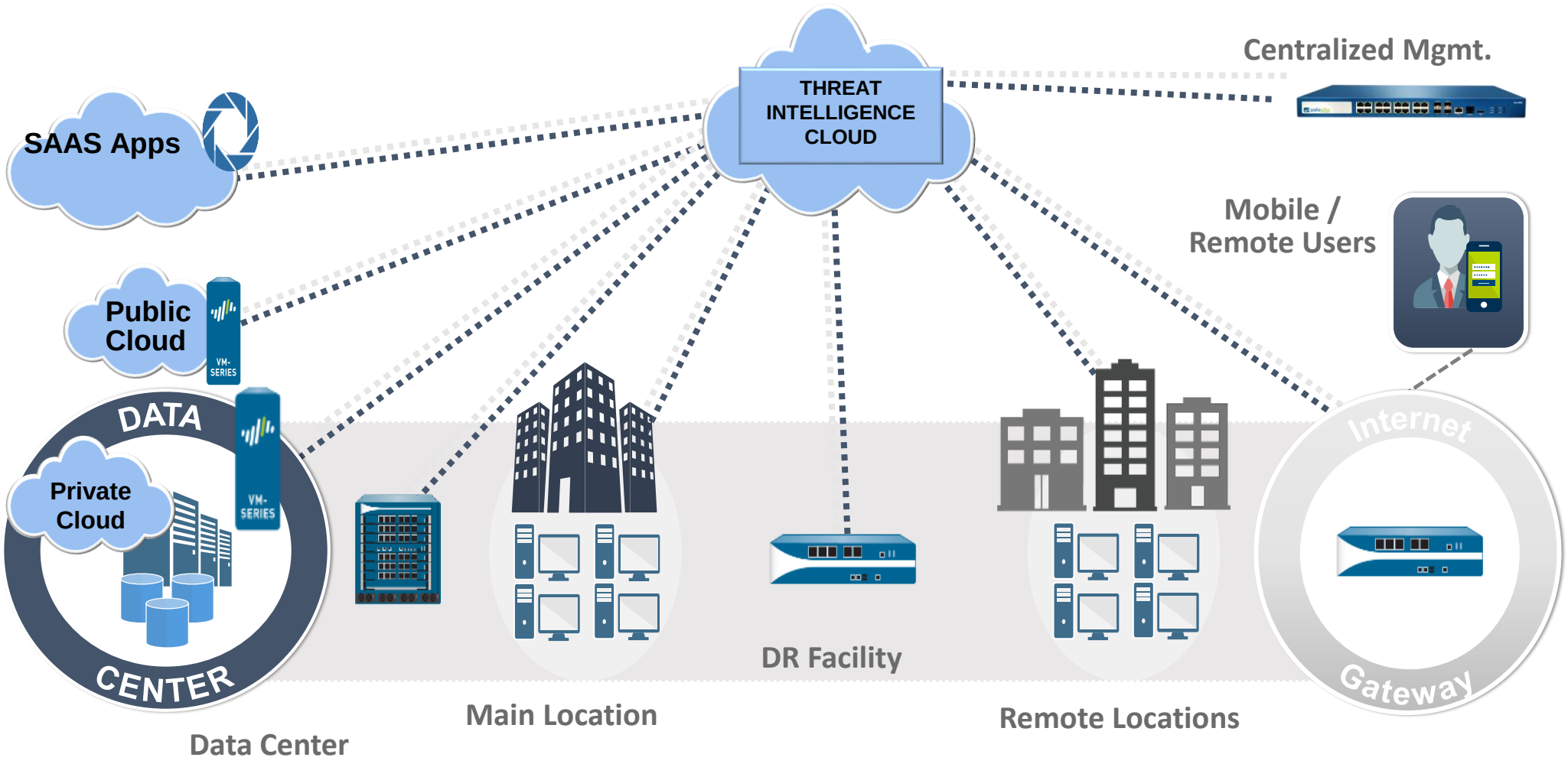
SLAIT Consulting

Other Threat Vectors

- What are you doing about Cloud Services?
- Are you containing mobile data movement?
- Do you have a Software Governance and Third Party Risk plan?

SLAIT Consulting

Cloud Enterprise Security



paloalto networks

Delayed Threats

- If you found a threat today would you know it was a threat?
- Are you only looking at the new files?
- Are you tenacious and unrelenting?

SLAIT Consulting

Q & A

SLAIT Consulting

Security Webinars at SLAIT

http://www.slaitconsulting.com/events

An **advanced persistent threat** (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity, typically for business or political motives. According to the InfoSec Institute, 2016 will be a year where the most serious threats for government and private businesses will come from cyber espionage. Nation state actors (APTs) - are well funded, increasingly sophisticated and extremely sneaky.

In this webinar, SLAIT's CISO, Arnold Bell, will address the current state of APT's and the techniques used by the more prolific actors and their shift in motivation. Attend to learn the best ways to defend your environment to prevent and/or minimize the damage that could be caused by APT actors.

SLAIT Consulting

SLAIT Security Solutions

Governance

- Risk Assessment
- Policy and Procedure
- PCI Prep
- HIPAA Gap Analysis
- Audit Preparation Assistance
- Security Organization Review
- Security Checkup

Prevention

- Managed Firewall and Endpoint
- Secure Infrastructure Design & Review
- vISO Program
- Awareness Training
- Assessment
  - Vulnerability Scanning
  - Penetration Testing
  - Phishing Exercises

Response

- ThreatRecon
- Pre-breach Preparation
- ThreatManage
- Breach Response
- Cyber Forensics

Technology Partners

Bit9 + CARBON BLACK ARM YOUR ENDPOINTS.

BlueCoat

paloalto NETWORKS

zscaler Secure. Everywhere.

splunk>

FireEye

websense ESSENTIAL INFORMATION PROTECTION

f5

aruba NETWORKS

SLAIT Consulting

Thank you for coming

Interested in seeing how SLAIT can help you?

Please come talk to me at the end or take a business card

SLAIT Consulting

References

- https://en.wikipedia.org/wiki/Defence-in-depth_(Roman_military)
  - Yeah, I know – its Wikipedia!
- http://searchsecurity.techtarget.com/definition/defense-in-depth

SLAIT Consulting