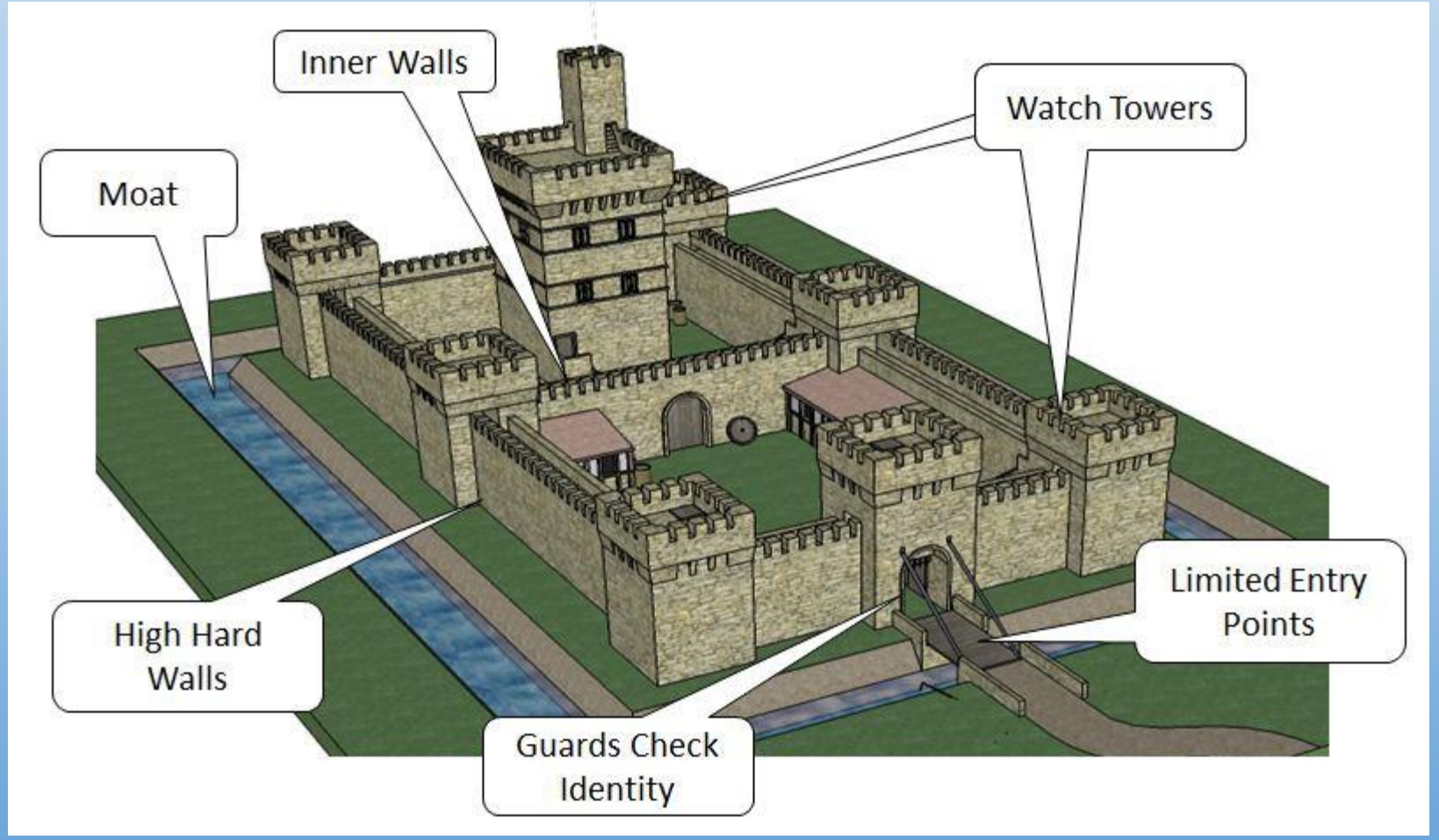
We Purchased the Best Protection Money Can Buy! Breaches are Still Everywhere! What Now?

Luis Brown, CISSP, C|CISO

Everybody Uses Protection:

- Firewalls – your basic lock
- Intrusion Protection System – large dog or aggressive cat
- Threat Intelligence – pictures of the bad guys + local police
  - Web Security / Proxy Server
  - Email Security / Threat Extraction + Emulation Analysis
- Endpoint Protection – homeowner with a club
- Web Application Firewalls – hopefully?

Layered Defense is based on the Ancient Model



And Yet…

- We still don’t protect us from us!

Central New Mexico Community College

Common Sense Approach?

- Risk Assessment
  - Too Many Risk Assessments are really “Threat Assessments”
  - Make sure you classify assets and determine which assets to protect
  - Blanket protections can result in “noise” unless you have unlimited staff
  - Targeted protections against “known threats” must be augmented
- Security Professionals must become Business Professionals and align with strategic business goals

Verizon says…

- Current High Priority Threats

Threat	Type of Data	Effectiveness	Score	Value
Payment Card Skimmers	PCI	84.3%	42.2%	Low
Web App Attacks	PII	17.0%	17.0%	High
Miscellaneous Errors	PII	1.7%	1.7%	Low
Insider and Privilege Misuse	PII	1.6%	1.6%	High
Physical Theft and Loss	PII	0.6%	0.6%	Low
Crimeware	PII	0.6%	0.3%	Low
Denial-of-Service Attacks		0.0%	0.0%	High
Point-of-Sale Intrusions	PCI	98.3%	0.0%	Low
Cyber-espionage	PII	62.8%	0.0%	High

- Threat data compiled using the Verizon Data Breach Report for 2015
- PCI – Payment Card Institute (Credit Card Data), PII – Personally Identifiable Information

CNM
Central New Mexico Community College

Gartner says…

- Gartner suggests that the future is in Detection and Remediation (D&R)
  - 15% of security budget spent on D&R should grow to 60% in 5 years
- Very little is spent on detection or incident response
    - UNLESS there is an incident!

Security Awareness & Training

- Basic Security Awareness
  - Most organizations require annual training
  - While this “checks the box”, it doesn’t actually do much
- REAL Security Awareness
  - Is done on a continual basis – perhaps randomly
  - Includes alerts when a campaign is underway
  - Is NOT effective without assessment
  - Which Means: Phish/Vish/Smish ourselves
  - Gather analytics and use them

Detection:

- The vast majority (>80%) of data breaches begin with credential theft
- We must increase visibility into our organizations to detect credential compromise
- Possible solutions
  - Deception systems - modern honeypot technologies – landmines anyone?
  - Multi-factor authentication – are your really who you say you are?
  - User Entity Behavioral Analysis (UEBA) – we are watching you?
  - Machine learning – both supervised and unsupervised
  - User Processes – Skimmers can’t work if they are found during routine inspections
  - Security Event Information Management (SEIM) – becoming less relevant? Good forensics tool…

Response:

- Most have an incident response procedure
  - Generally not followed well during an incident
- Too many inconsequential incidents
  - Most incidents with current systems are false alarms
  - Tend to become routine and mostly ignored
  - Remember Target!
- Good Detection and Correlation reduces false alarms and minor incidents
  - Machine evaluation of incidents makes response more effective

In the end we must persevere…

Questions? Rebuttals? Comments?

CNM
Central New Mexico Community College