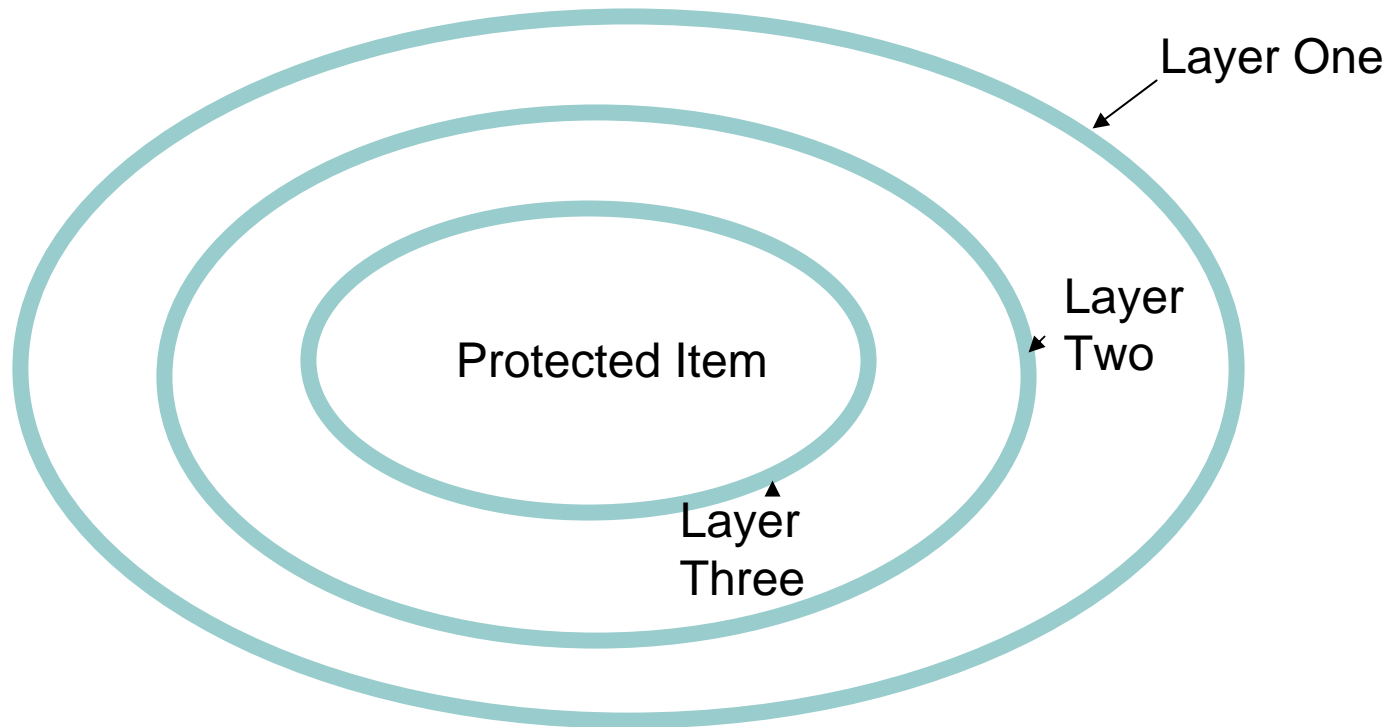


Defense in Depth





Castles

- The embodiment of Defense in Depth
- Have proven the usefulness of layered defense
- Rely on multiple defenses



Building a Network Castle

1. Comparison between IS and Castles
2. Three concerns for building a castle
3. Building a castle, but not breaking the bank
4. Evaluating a system
5. Tactics for implementing Defense in Depth

Castles and IS

○ Castle

- Defend valuables
- Base of operations
- Extend Power
- Hub of Commerce
- Expensive

○ Information Systems

- Defend data
- Key to system operations
- Leverages the power of the company
- Hub of intellectual and virtual commerce
- Expensive



Three Concerns for Building a Castle

- Location
- Access
- Man-Power

Location

○ Castle

- Proximity to Trade Routes, Communities
- Proximity to Resources
- Area adequate to house a castle

○ Information Systems

- Space
- Power
- Storage
- Real Estate



Access Control

- Castles

- Walls
- Moats
- Towers
- Weapons
- Internal Walls

- Information Systems

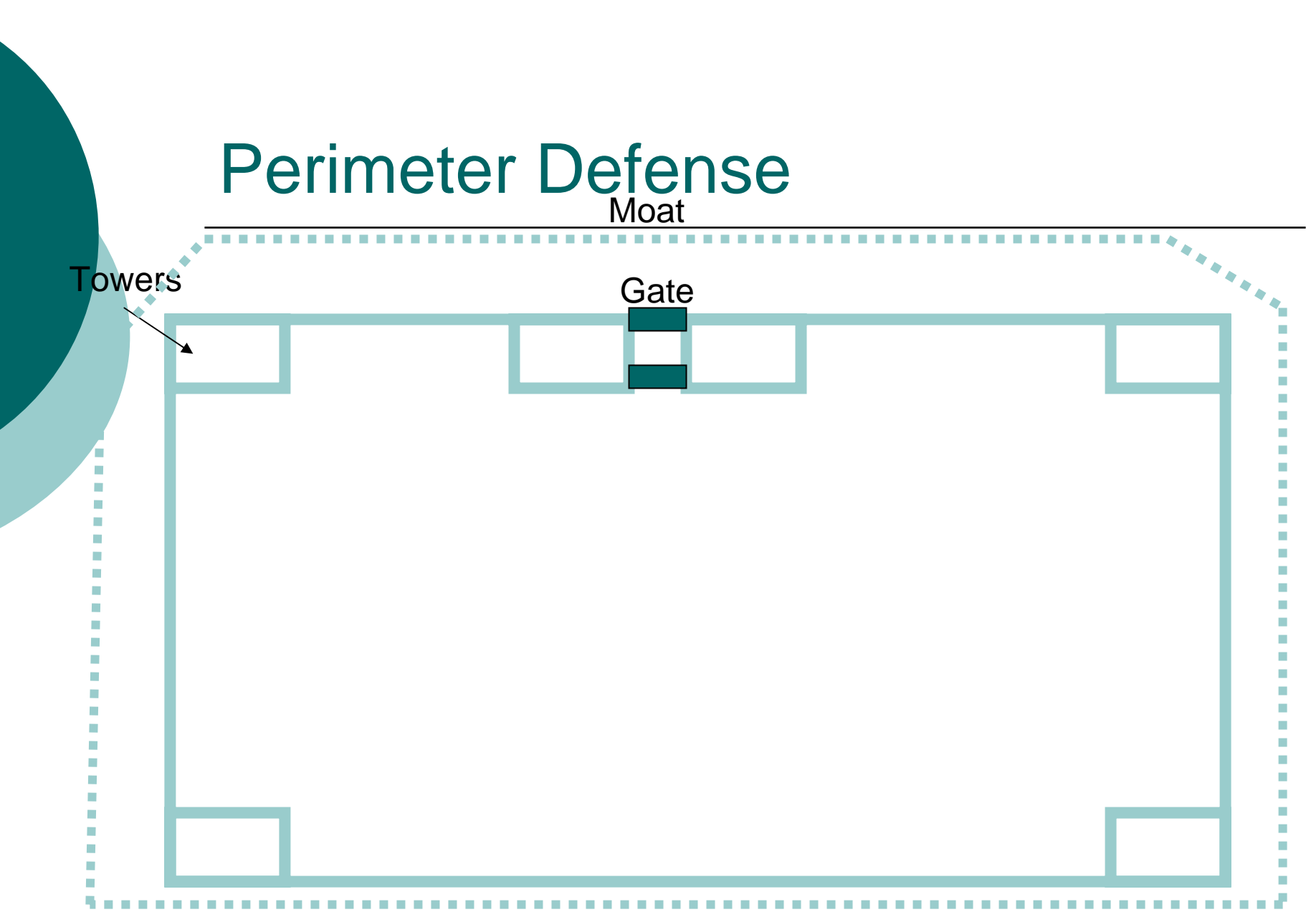
- Perimeter Defenses
- Secondary Defenses
- Internal Controls

Perimeter Defense

Moat

Towers

Gate



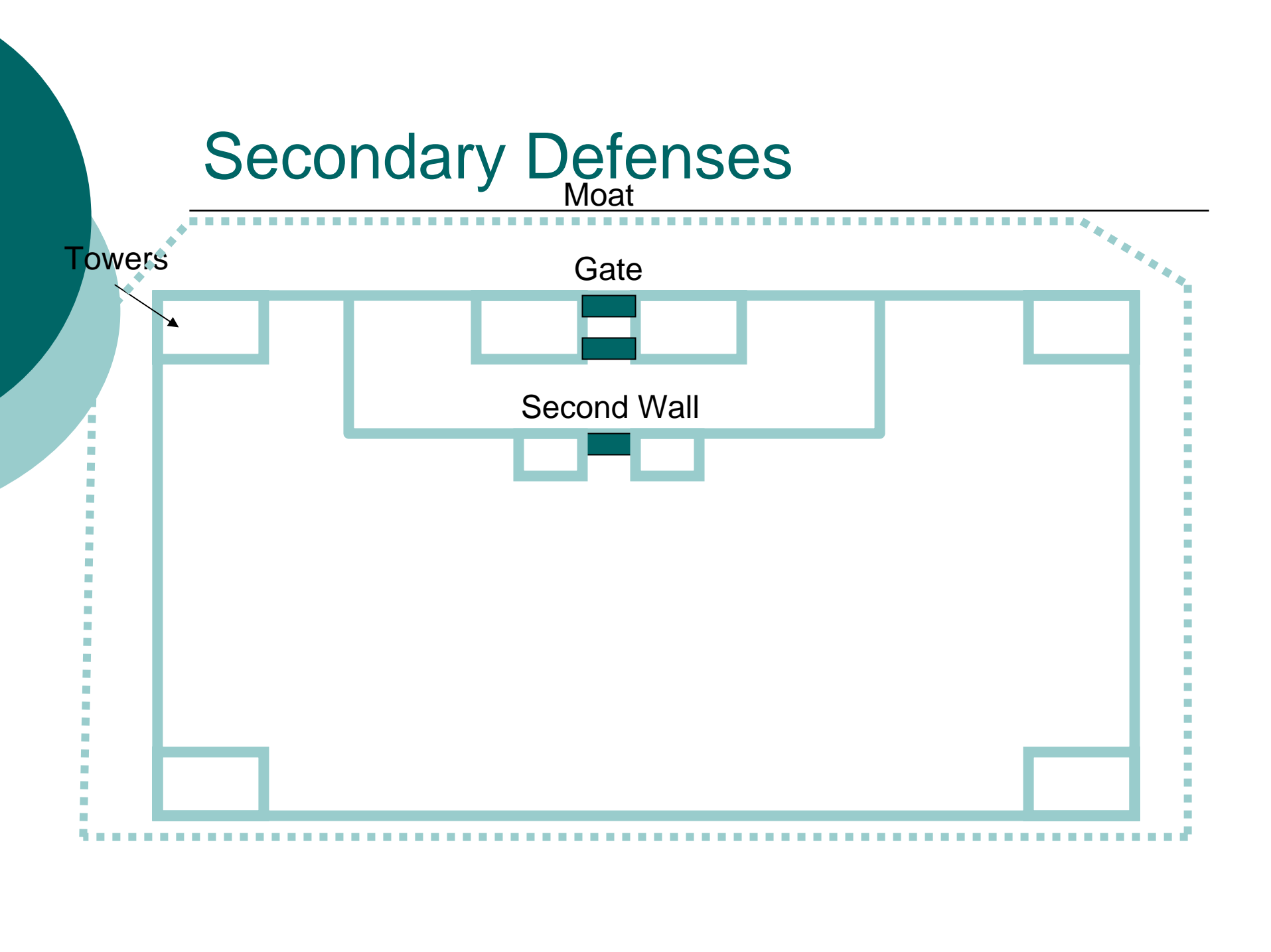
Secondary Defenses

Moat

Towers

Gate

Second Wall



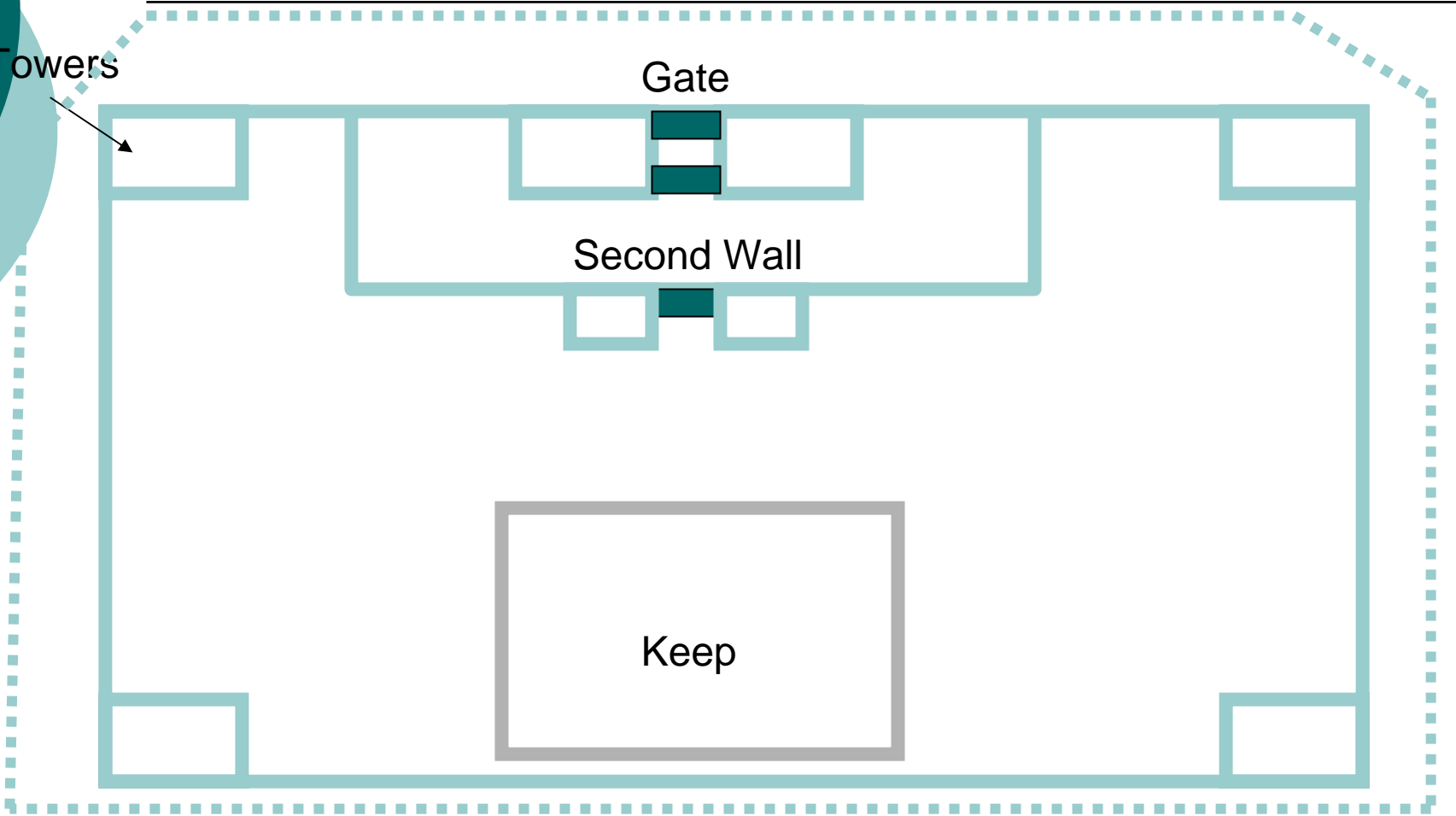
Internal Controls

Towers

Gate

Second Wall

Keep





Man-Power

- Castle

- Guards
- Patrols

- Information Systems

- Network Admin
- End users



Improving Man-Power for IS

- Training/Education
- Monitoring
- Policies



Building a Castle, Not Breaking the Bank

- Information Systems are:
 - Expensive
 - Large
 - Difficult to Quantify
- It is necessary to evaluate a System



Value the IS Assets

- List all assest to the system (data included):
 - Importance to organization
- Determine Value
 - Impact to organization if lost
 - Cost to repair
 - Repercussions
- Value = Importance
(Impact + Repair + Repercussion)

Determine Risk

- Likelihood
 - What is the probability of a an attack upon an Asset
 - Score from 0 to 5
- Severity
 - What is the likely damage of an attack upon an Asset
 - Score from 0 to 5
- $\%Asset_Risk = (Likelihood + Severity)/10$

Determine Residual Risk

- Residual Risk is the level of Risk for an Asset.
 - Summing Residual Risk for all assets should give total organizational Residual Risk.
 - The cost for Safeguards and Counter Measures is deducted from Residual Risk.
 - Residual Risk should never be negative, or too low as such implies spending too much on defense.
- $\text{Residual_Risk} = (\text{Asset_Value} * \text{Asset_Risk}) - \text{Safeguards}$



Evaluation Goals

- Identify Valuable Assets
 - Counter measures can be concentrated on them.
- Quantify the value of assets
 - \$ figures for defense
- Focus Design to meet organization



Growth:

- Always determine how much growth is expected in the company over the next several years.

Power Requirements

- Always examine the power requirements of a proposed system as well as the wiring at a given site. Include in all plans a backup generator. If the building is old, budget enough for rewiring. If the location is set, make certain that power output is adequate and work on getting the best UPS within budget.



Network Infrastructure

- When building a new system, plan for speed and bandwidth, but don't go overboard. Fiber to every workstation might sound like a great idea, but the cost and problems installing it would prove a headache. If the wiring is old, think long and carefully before rewiring the building.



Software Resources

- Software licensing is expensive and often many employees use only a small portion of the applications that come bundled on their PCs.



Maintain Documentation

- Document the Design of the network, and update that documentation as changes are made. This document should be accessible to those that manage and administer the system.

Evaluate the Organization's Data needs

- Follow the evaluation procedures above and identify the most valuable assets of the system. Make certain that those assets have greater protection in the design. Maintain this documentation and update it as changes occur.



Build a disaster Recovery and Archival plan

- Clearly Document and plan archival of the network. Include testing in the plan to make certain the archival process works. Further, build a Disaster Recovery plan, and diversify system resources so that a single disaster will not wipe out all data.

Document Users

- Always maintain an up-to-date list of all employees, their user names, job title, and permissions. This document should be updated, at the very least, any time there is a change in staffing. This document can be used as the list of valid usernames/privileges when monitoring the network.



Maintain constant Virus Protection and Monitoring!

- Enough Said



Practice the Policy of Least Privilege

- Give users the bare minimum to accomplish their jobs. This practice can be exhaustive to Network Administrators as it will incur a large number of phone calls from angry users, but it will help reduce the number of users on the system with inflated privileges and make it easier to track them. Further, this forces the users to legitimize their need for a system resource.



Learn scripting

- Perl scripting, in particular, is a powerful tool that can be used to manage a system. A few well crafted Perl scripts could rapidly identify users not in the documentation, rogue accounts, and other anomalies.



Use firewalls liberally

- Firewalls do not need to exist only in the DMZ. Place them within the internal network whenever you wish to further protect valuable system assets.



Harden all Servers

- Do not run a service unless it is needed. Operating systems like Open BSD can give the system a little extra protection as the default install has few services running.



Encourage fewer good passwords rather than many poor ones

- Password guessing is one of the easiest way into a system mainly because it is difficult to remember many passwords. Where possible use single logon with strong password rules.



Use software

- There are thousands of tools that all help with the management and monitoring of networks. Some tools are horribly expensive, others don't cost a dime, but take a while to learn. Invest some time and effort and determine which ones work within budget and time constraints.

Training

- Budget money for the IT staff to train in the technologies at the business. Offer incentives for those that train on their own time. Ultimately, the better trained the IT staff, the better able they will be able to administer the system. Simply setting aside a couple hours a week for the staff to train internally could have a dramatic effect.



Build a lab

- Labs are a great way to practice and evaluate threats, to test patches and upgrades, and to learn. Throw together a small number of PCs networked together, but disconnected from the system network. Spend some time every week/month to learn about current vulnerabilities, or to test software. This type of education is exceptionally valuable to the IT staff.



Education, education, education

- Teach end users that their actions can compromise the system. Most of this education can be done internally and should be geared to raising awareness. Make certain to address the perils of social engineering.

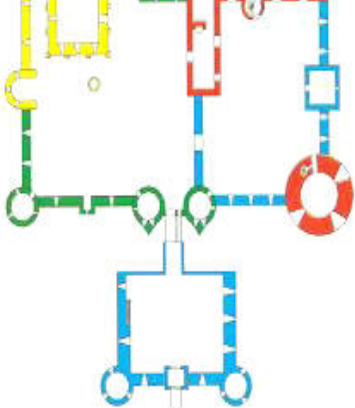


Create Policies

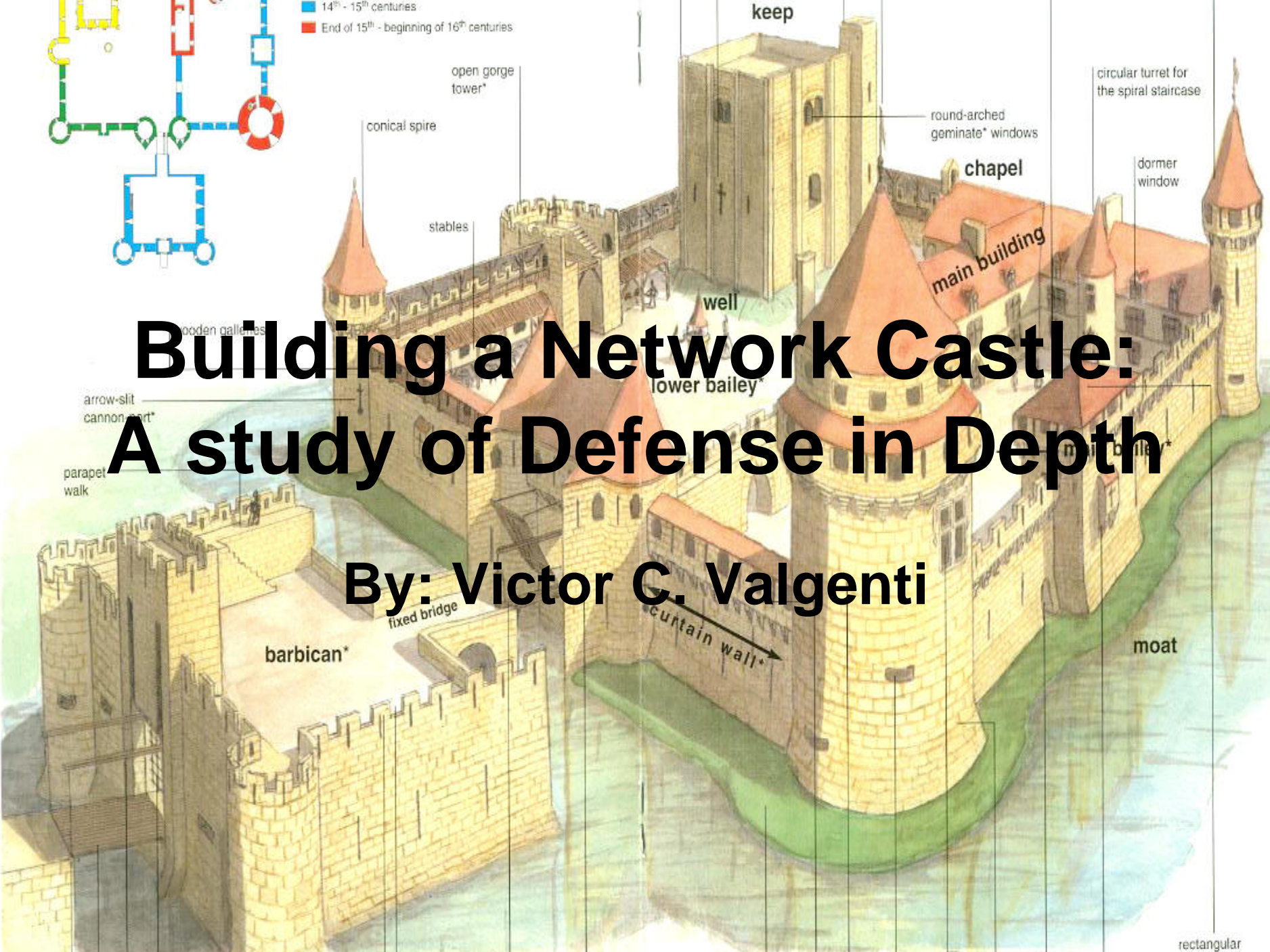
- Create a policy for anything that gets done on the system. Make certain that all employees are aware of these policies and have signed off on them. Further, allow for change in these policies as the environment changes.=

Bibliography

- Creighton, Oliver H., *CASTLES, LORDSHIP AND SETTLEMENT IN NORMAN ENGLAND AND WALES*, History Today, Apr2003, Vol. 53 Issue 4, p12.
- Paul, Brooke, *BUILDING AN IN-DEPTH DEFENSE. (Industry Trend or Event)*, Network Computing, July 9, 2001 p75.
- Johnson, Johna Till, *Security today means playing 'defense-in-depth'.*, Network World, August 16, 2004 p24.
- Johnson, Johna Till, *Figuring out Information Stewardship*, Network World, August 9, 2004.
- Jackson, William, *ONI counts on defense-in-depth, redundancy for its nets. (Technology Report)*, Government Computer News, Feb 9, 2004 v23 i3 p25(1).
- Salloum, Habeeb, *Syria's Crusader Castles.*, Contemporary Review, Jan2000, Vol. 276 Issue 1608, p28, 5p.
- Sixth Workshop on Education in Computer Security, Naval Postgraduate School, Monterey, CA, July12-16, organizers and presenters: Cynthia Irvine, Naomi Falbi, J.D. Fulp, Mathew Rose, Daniel Warren, Blaine Burnham, George Dinolt, Deborah Frincke, Tim Levin, Bill Murray, and Giovanni Vigna.
- Castle Picture from About.com



14th - 15th centuries
End of 15th - beginning of 16th centuries



keep

circular turret for the spiral staircase

round-arched geminate windows

chapel

dormer window

main building

well

lower bailey

conical spire

stables

open gorge tower*

wooden galleries

arrow-slit cannon port*

parapet walk

By: Victor C. Valgenti

barbican*

fixed bridge

curtain wall*

moat

rectangular (for four-sided)