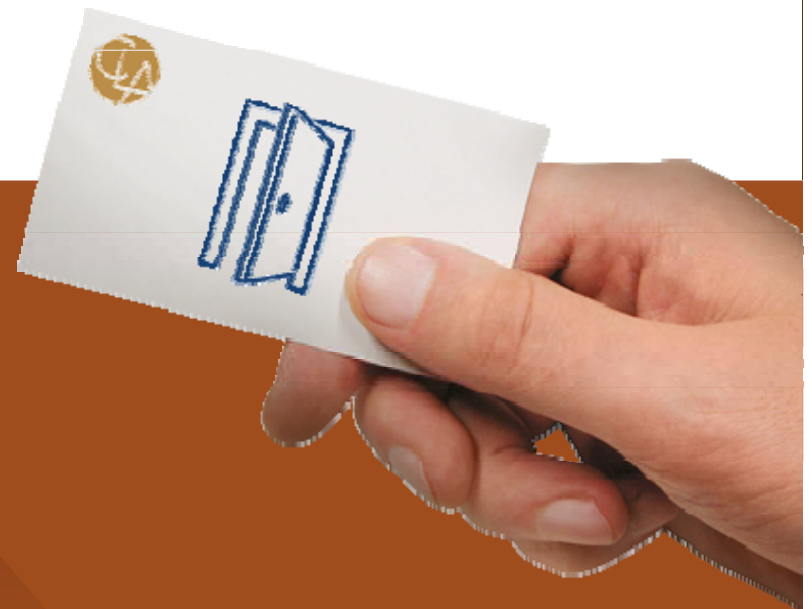


# Physical Security to mitigate Social Engineering Risks



**CliftonLarsonAllen**

[cliftonlarsonallen.com](http://cliftonlarsonallen.com)



# Agenda

- Background and statistics of physical security
- Address social engineering risks associated with deficiencies in physical security
- Explain attacker motivations
- Identify sound physical security measures to protect critical assets
- Summarize key areas of control your organization should have in place to improve the security posture

## Physical Security- It's kind of a big deal...

- The worldwide market for physical security was valued at \$48 billion in 2012 and is projected to reach the market size of \$125 billion by 2019<sup>1</sup>.

<sup>1</sup> <http://www.transparencymarketresearch.com/physical-security-market.html>

## And the winners are...

- Video Surveillance was the largest market and held about 72% share in 2012 with a forecast to continue that rapid growth<sup>2</sup>
- Biometrics held the largest market and held about 38% share in 2012<sup>3</sup>

## Trivia time...

What industry is the largest end-user of physical security?

2, 3 <http://www.transparencymarketresearch.com/physical-security-market.html>

# Identify what needs to be protected



## Defense in Depth

- The concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack.
- ***Not enough to just secure your network***



# Social Engineering Risks

---

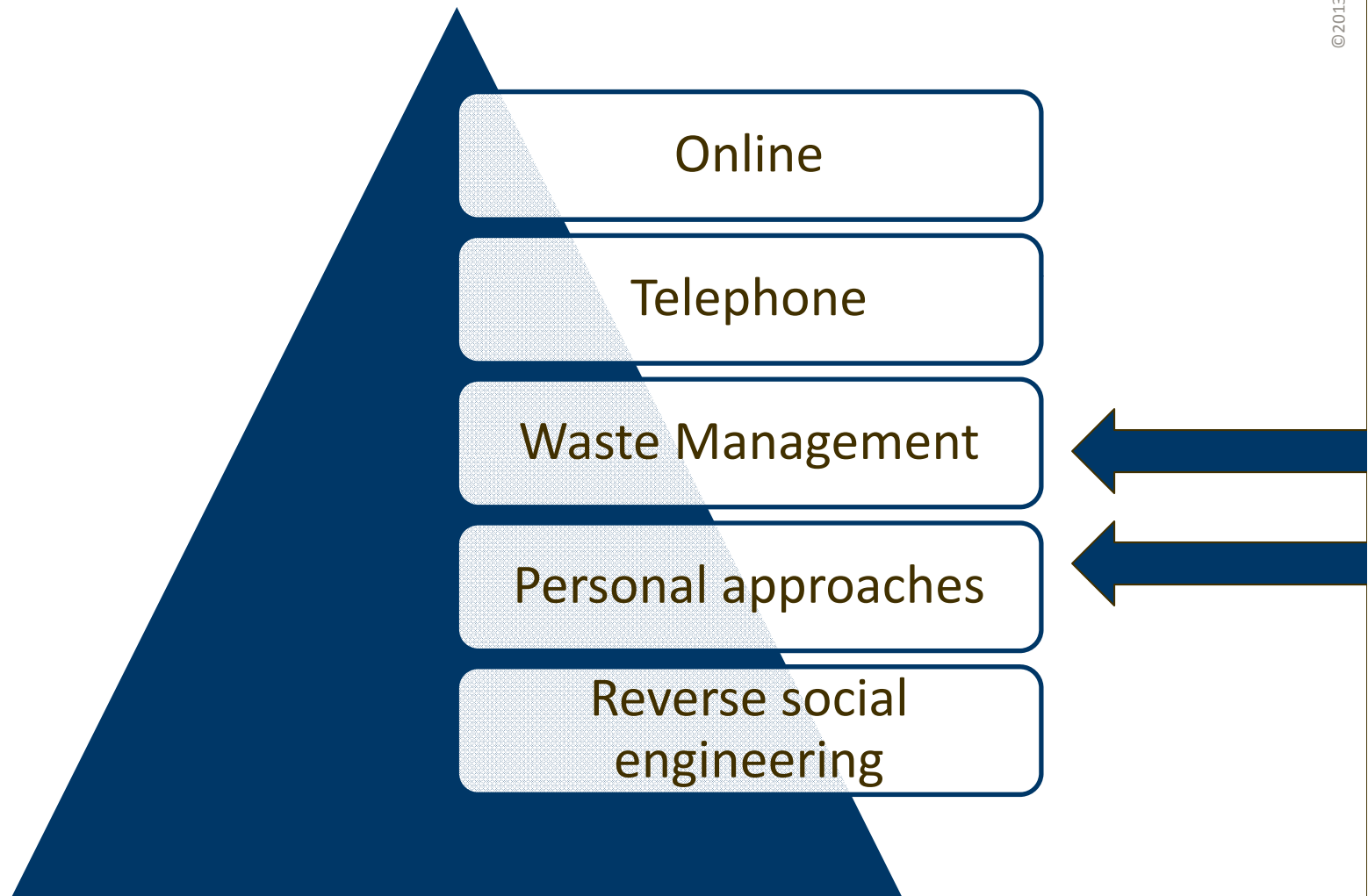
# Social Engineering

- Hacking the human
  - Simply put, Social Engineering is the exploitation of human nature.
- Highest risk for these attacks?
  - New employees [60%]
  - Contractors [44%]
  - Executive assistants [38%]





# Several different attack vectors



## Recon... Google it

- The *information gathering* process is critical. The internet can provide a host of information essential to performing a successful social engineering attack
- Google images
  - Facility access, entrances
  - Type of access control used
  - Employee information
- Information is a dangerous weapon. Adds legitimacy where there is none

# Tailgating

- Gaining access to a physical access facility by means of coercion or manipulation or simple entry
- Total bypass of physical security
- Employees and vendors avoid confrontation
- Attributed to deficient or lack of access restriction, lack of security awareness

***“Cigarettes are a social engineer’s best friend.”***



# Shoulder Surfing

- Direct observation
- Effective in public areas
- Access to confidential information
- Attributed to deficient privacy features, improperly restricted areas



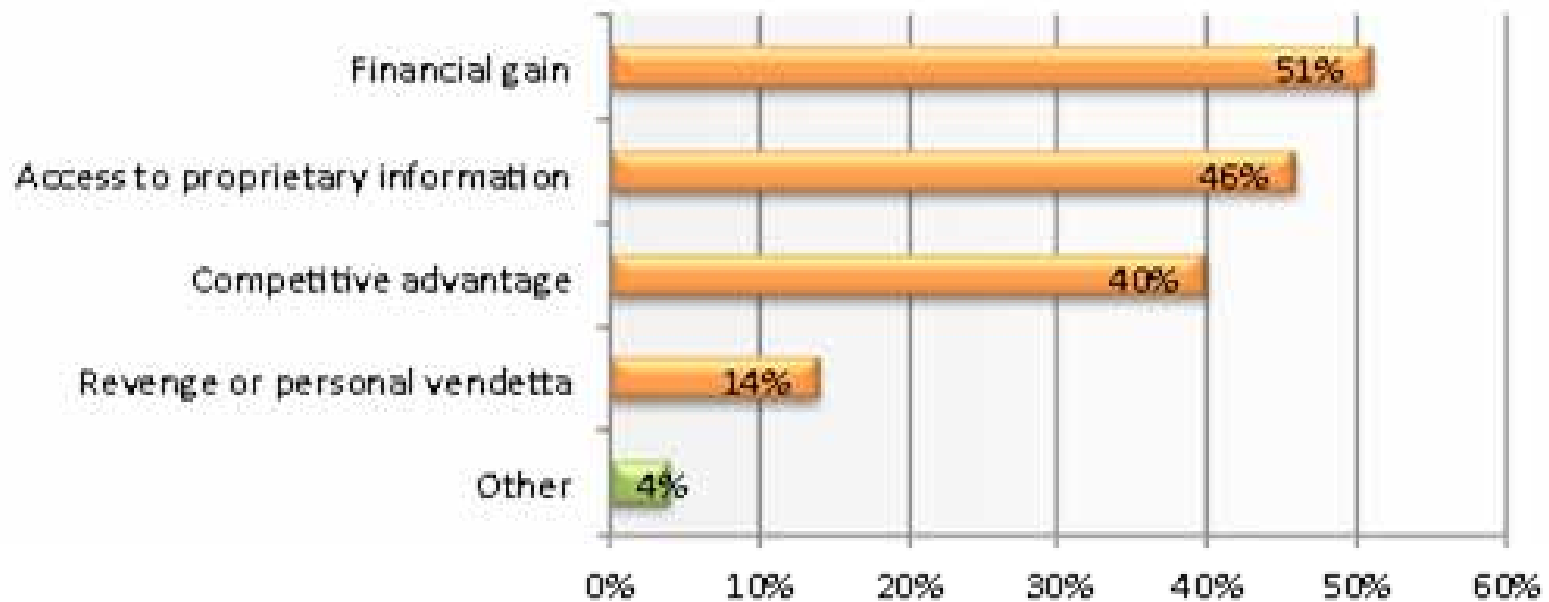
# Dumpster Diving

- Looking for information discarded by company employees
- Typically done after hours
- Reconnaissance has likely been done prior to attack
- Attributed to lack of access restrictions, deficient disposal procedures



***“One man’s trash is a social engineer’s treasure.”***

# Motives



## Motivations for social engineering attacks

- Other motivators include knowledge, curiosity, ego, social acceptance and pure entertainment (base jumping)



# Defensive measures to prevent Social Engineering attacks

# Types of Physical Security

- Intrusion Detection/Prevention
  - Alarms, Video Surveillance
- Access Control
  - Locks, Access control, Visitor control



# Video Surveillance

- Video Surveillance is one of the oldest physical security measures available
  - Now running on same IP network as other apps
  - Must be securely configured
  - Real time monitoring
  - Unattended cameras simply aid in forensics
- Placement is key
  - All entrances, work areas, inside and outside of data center

# Alarms

- Perimeter and Internal
  - Various sensors can be implemented
  - Police response
  - Time of day restrictions can be enforced
  - Alarm codes should be unique for each employee
  - Access is restricted using ACL

# Access Control, it's not just an IT problem

- Relationship with facility management
- Access review should occur regularly
- Time of day restrictions
- Layered security
- Discuss options with vendor



# Radio Frequency ID Cloning (RFID)

- 3 levels of frequency
  - Low (LF) cloned within 3 ft
  - High (HF) cloned within 3-10 ft
  - Ultra-High (UHF) cloned within 30 ft
- Most access control utilizes passive low frequency RFID technology
- Discuss options with vendor

## Locks

- Virtually any key lock can be picked
- If you **MUST** have key locks, implement additional controls
- Inventory of keys needs to be maintained
- Electronic locks are best
- Access codes should be unique for each employee
- Access is centrally managed



# Visitor Control

- Guards
  - Human eyes are often better
- Visitors announced and escorted
- Sign visitor log
- Wear visitor badge (preferably automated access control)
- Implement compensating controls

## Controlling Paper

- Locked shred bins
- Vendor picks up and shreds onsite
- Certificate of destruction is provided
- Clean desk policy
- Random walkthrough for compliance
- Employee awareness
- Secure dumpster area

# Summary

- Layered security is best
- Security is a culture
- Validate your security
- Security awareness is key





## Pete Storm

Senior Associate, Information Security

Pete.Storm@claconnect.com

612-397-3070

## Laura Faulkner

Manager, Information Security

Laura.faulkner@claconnect.com

267-419-1165



**CliftonLarsonAllen**

[cliftonlarsonallen.com](http://cliftonlarsonallen.com)



[twitter.com/  
CLA\\_CPAs](https://twitter.com/CLA_CPAs)



[facebook.com/  
cliftonlarsonallen](https://facebook.com/cliftonlarsonallen)



[linkedin.com/company/  
cliftonlarsonallen](https://linkedin.com/company/cliftonlarsonallen)