RSA Conference2015
San Francisco | April 20-24 | Moscone Center

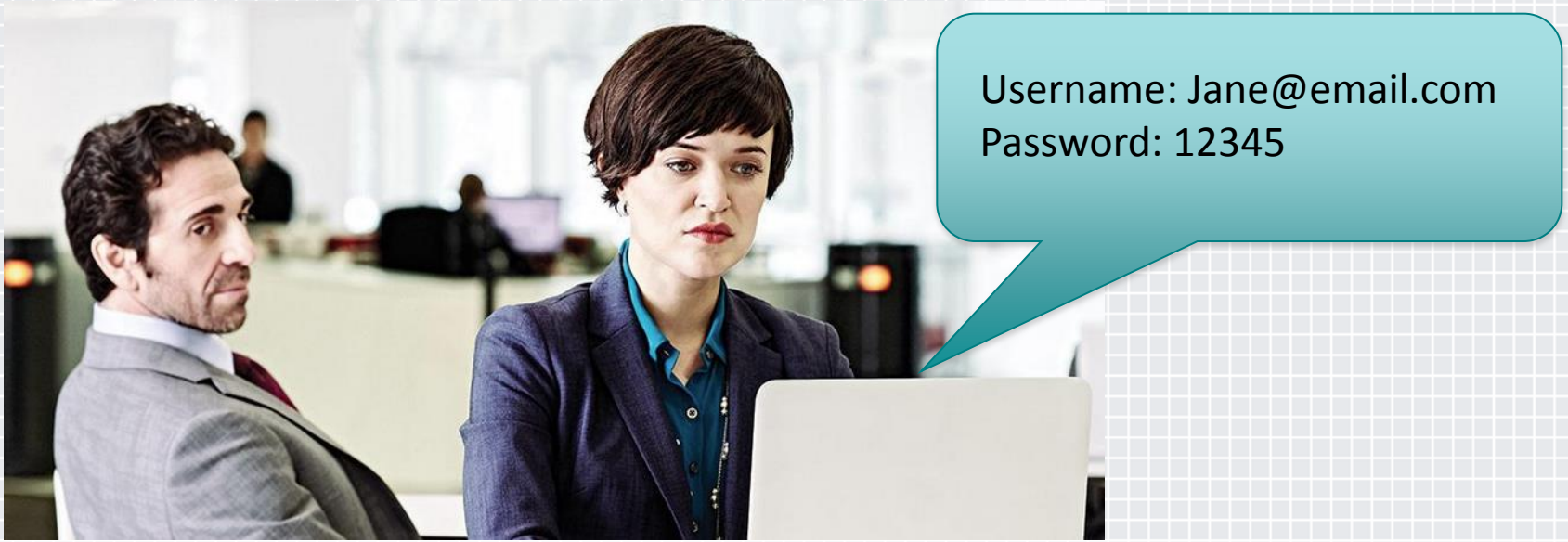
SESSION ID: HUM-R04

How One Smart Phone Picture Can Take Down Your Company

Dr. Larry Ponemon

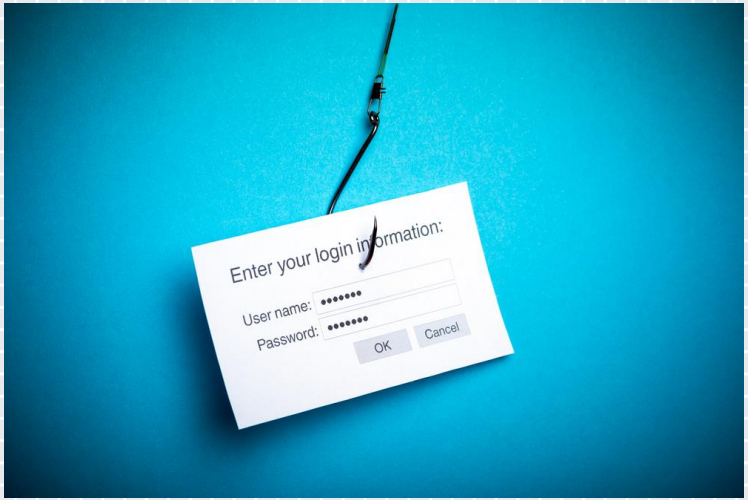
Chairman and Founder
Ponemon Institute
@Ponemon

Have You Ever Felt Wandering Eyes Over Your Shoulder?



What Are Some Common Low-Tech Threats?

- You've probably heard of low-tech threats like:
  - Social Engineering
  - Spear Phishing
  - Malicious Insiders
  - Physical Device/File Theft



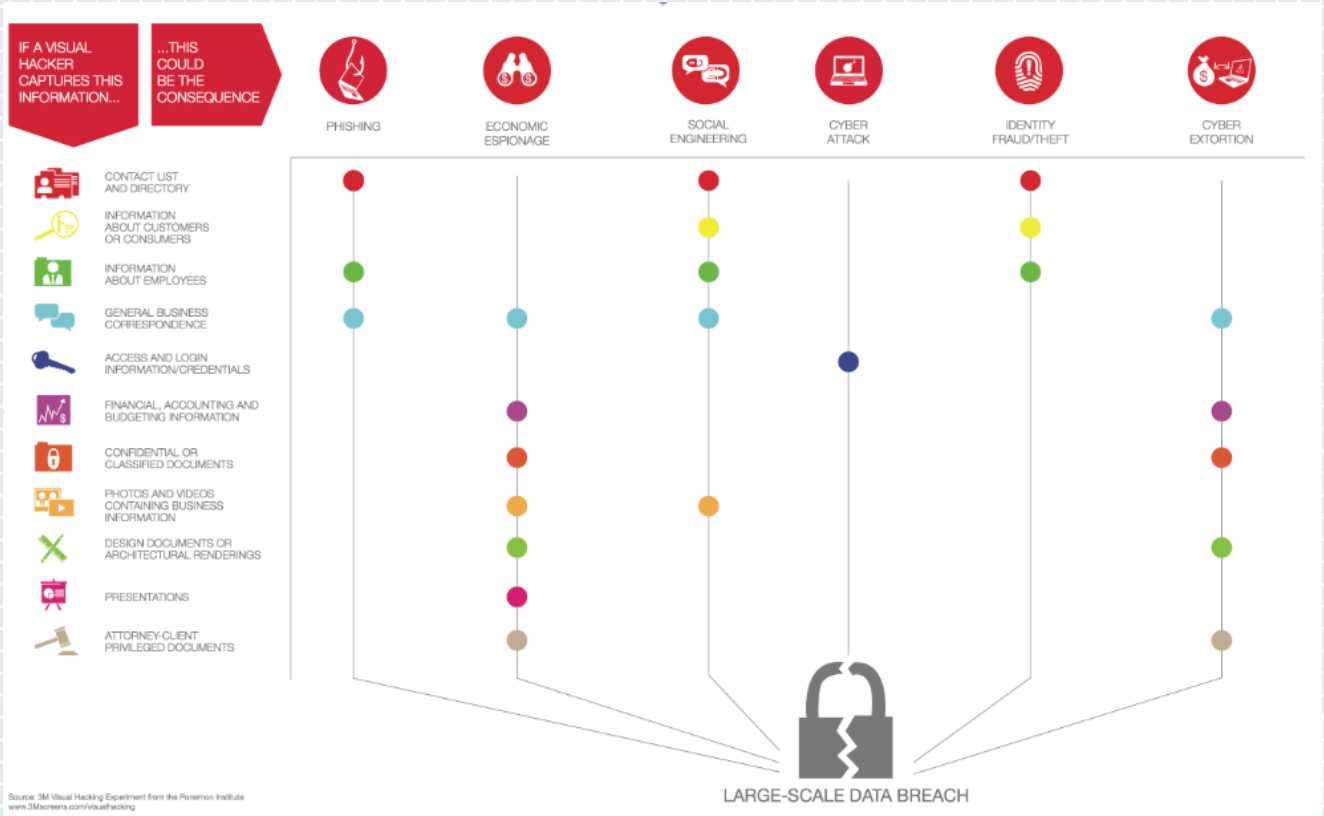
Visual Hacking: The Lurking Low-Tech Threat

- **Visual Hacking** is a fifth, under-addressed low-tech threat
- What is Visual Hacking?: A low-tech method used to capture sensitive, confidential and private information for unauthorized use
- What is Visual Privacy?: The act of protecting sensitive, confidential and private information from visual hacking
- **Informal Poll**: Raise your hand if this has ever happened to you

Why is Visual Hacking an Issue?

- Visual hacking is a weak point when protecting information through the pipeline (data in motion, data at rest, data in use)
- Visual hacking is a stealth threat vector, virtually untraceable
- As high-tech data security solutions become more and more sophisticated, hackers will shift from hacking systems to *hacking people*
- Visual hacking could be the gateway to a large-scale attack

The Path to a Large-Scale Data Breach



Examples of Visual Hacking Hotspots: In Office

Open Cubicles

Open-Office Floor Plans

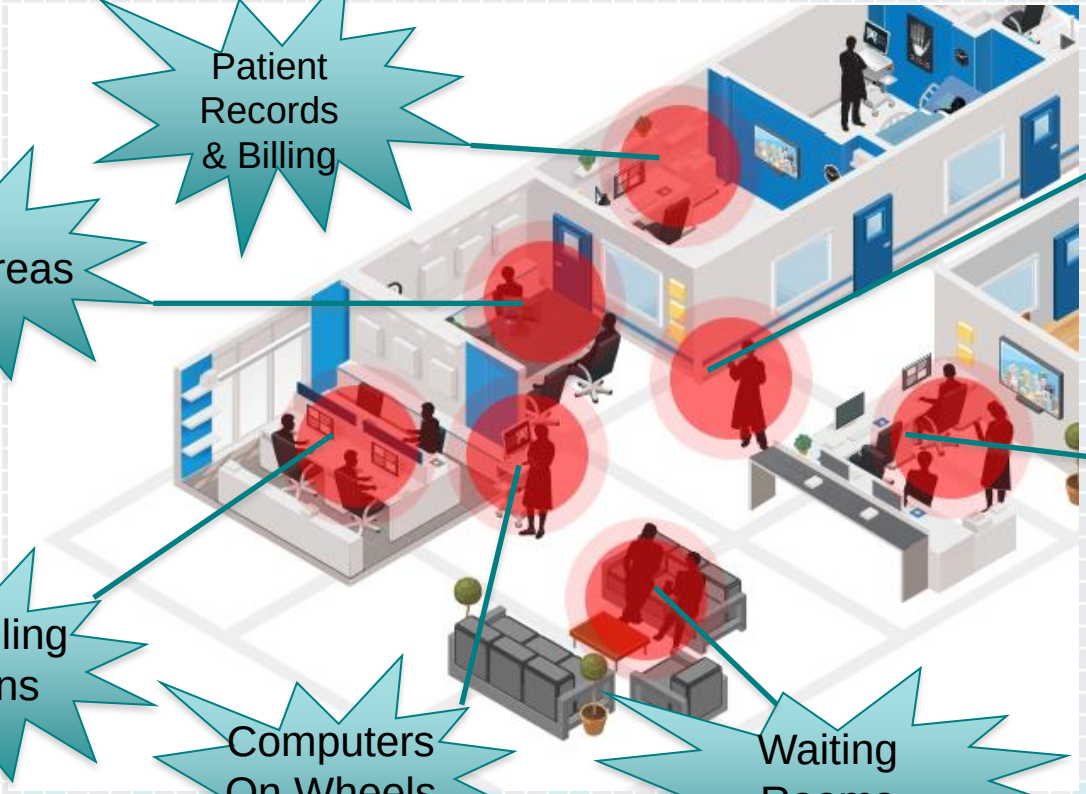
Tablets & Mobile Phones

Shared Workspaces

High-Traffic Areas

Waiting Rooms

Examples of Visual Hacking Hotspots: Health Care Setting



Patient Records & Billing

Physicians' Mobile Devices

Open Areas

Nurse Stations & Check-in Monitors

Scheduling Stations

Computers On Wheels

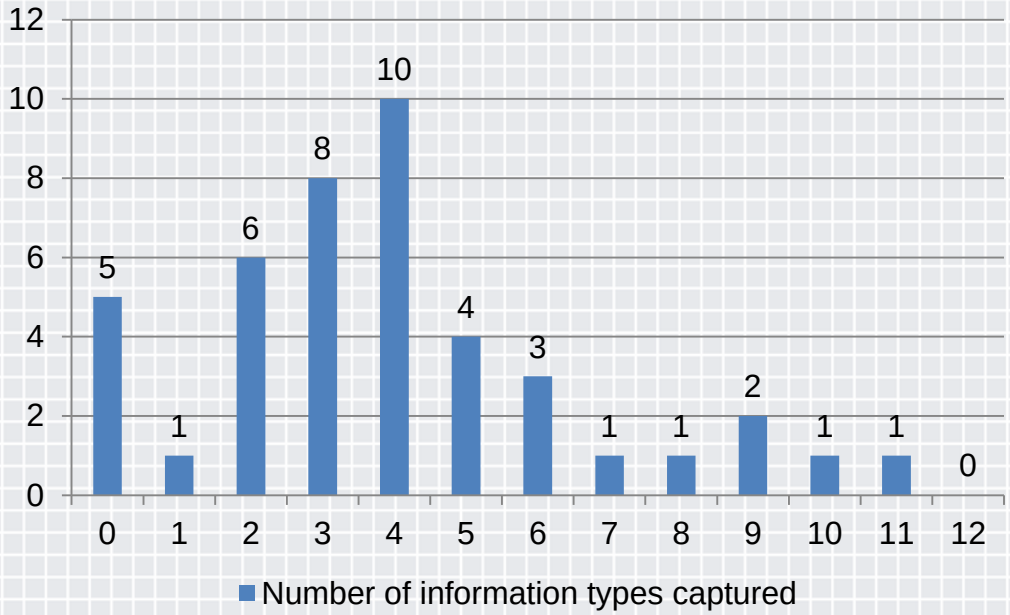
Waiting Rooms

RSAConference2015

San Francisco | April 20-24 | Moscone Center

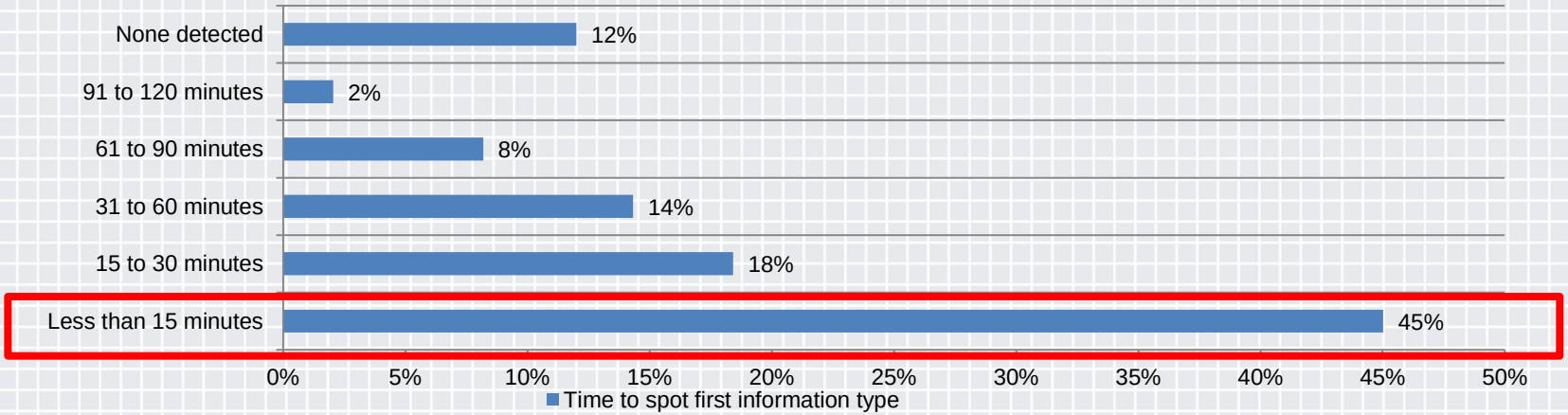
3M Visual Hacking Experiment Results

Being Visually Hacked is Not a Myth



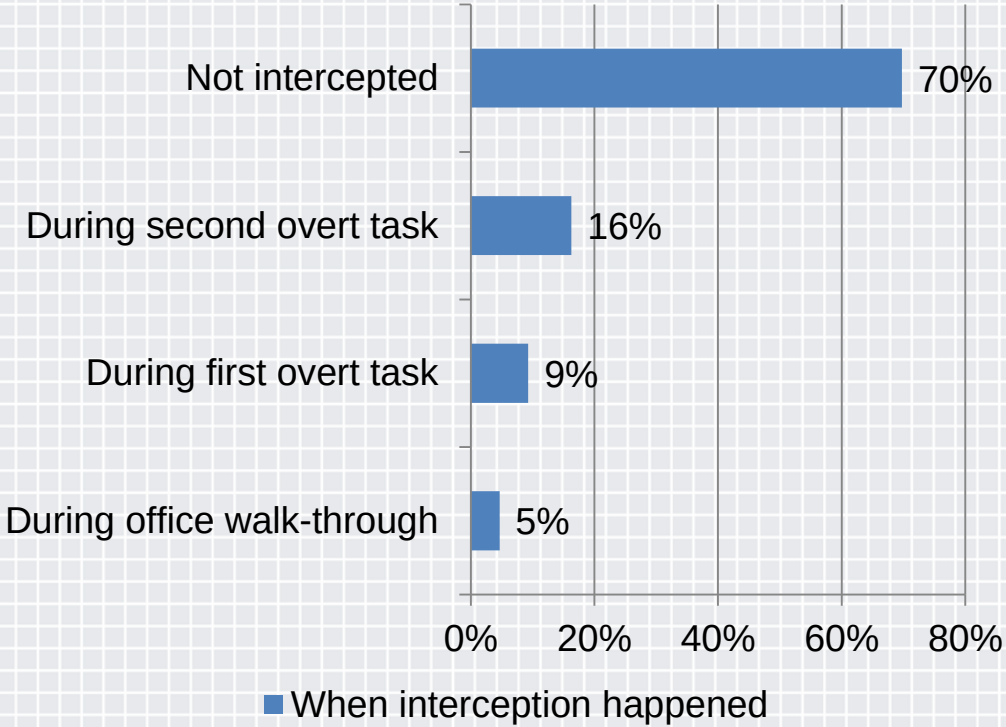
- In nearly **nine out of ten (88 percent) instances**, a white hat hacker was able to **visually hack sensitive corporate information**, such as employee access and login credentials

Visual Hacking Happens Quickly



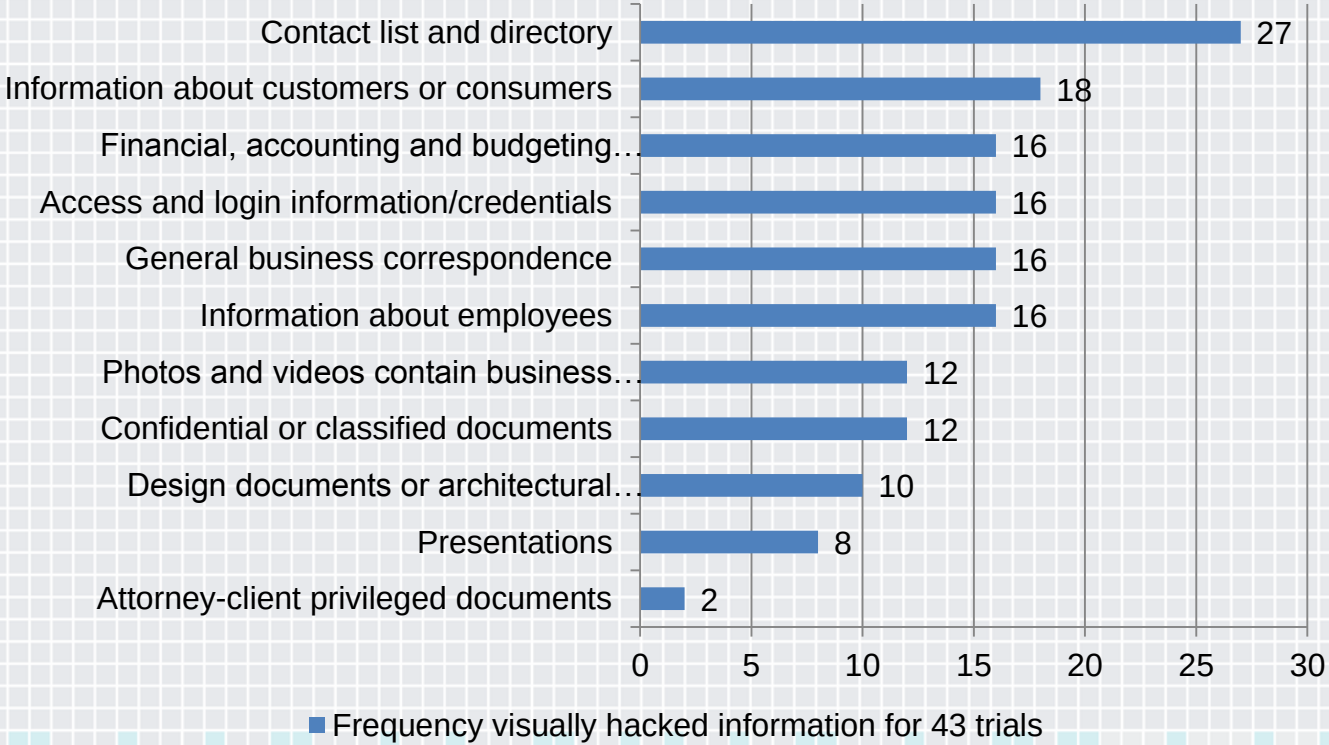
- Companies can be visually hacked in a matter of minutes, with almost **half (45%) occurring in less than 15 minutes**, and 63 percent occurring in less than a half-hour

Visual Hacking Can Go Unnoticed



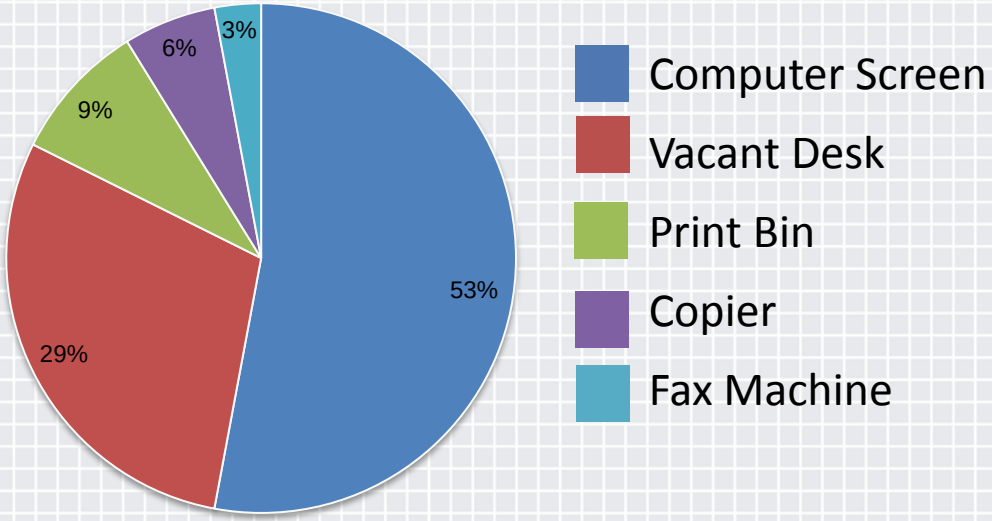
- In **70 percent of incidences, a visual hacker was not stopped by employees, even when a phone was being used to take a picture of data displayed on screen**
- In situations when a visual hacker was stopped by an employee, the hacker was still able to obtain, on average, 2.8 pieces of company information, compared to 4.3 pieces of information when not stopped

An Average of Five Pieces of Information Were Hacked Per Trial



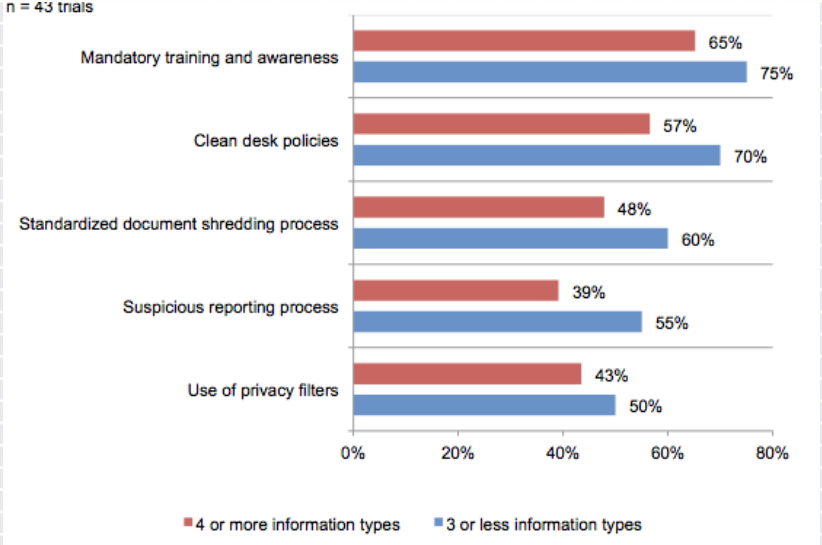
- During the experiment, an **average of five pieces of information were visually hacked per trial**, including employee contact lists (63%), customer information (42%), corporate financials (37%), employee access and login information/credentials (37%) and information about employees (37%)

Sensitive Information was Gleaned off Unprotected Devices



- **53 percent of information deemed sensitive**, including access and log-in credentials, confidential or classified documents, financial and accounting information and attorney-client privilege documents, was gleaned by the visual hacker from an **unprotected device**
- This is greater than information gleaned from desks (29%) printer bins (9%), copiers (6%) and fax machines (3%) combined

Visual Hacking Controls Help

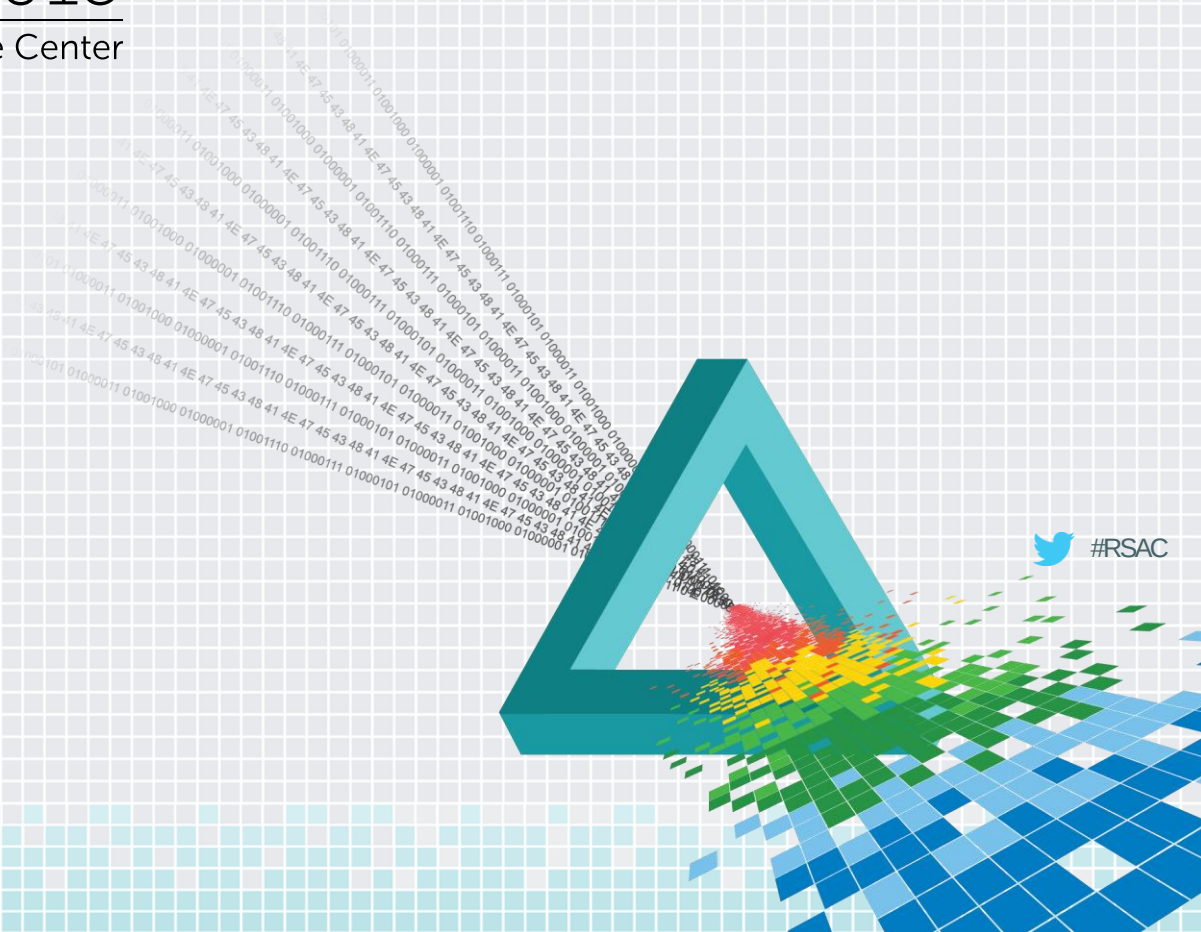


- In all instances, **those companies that employed visual hacking controls**, including mandatory training & awareness, clean desk policies, standardized document shredding process, suspicious reporting process and use of privacy filters**, had fewer pieces of information hacked than those that did not**

Conclusions

- Visual hacking is an under-addressed corporate risk with potentially detrimental consequences
- A hacker often only needs one piece of valuable information to unlock a large-scale data breach. This study exposes both how simple it is for a hacker to attain sensitive data using only visual means, as well as employee carelessness and a lack of awareness to data security threats
- Low-tech threats, such as visual hacking, can be as detrimental to companies as high-tech threats

Case Studies



Global Management Firm

- Business Case
  - Many consultants travel or work from client's offices regularly
  - A partner was on a plane traveling to a client. On the computer screen in clear text were client-attorney privileged documents and one of the firm's clients just happened to be seated next to the partner. The client contacted the firm's legal department and filed a complaint
  - Chief Compliance Officer: "There is growing awareness among the consultants about the social engineering risk that occurs during travel**. Many were not aware that potentially a cyber criminal whose sole purpose is to obtain credentials and personal information could be in the next seat.**"
- Solution
  - Privacy and data protection practices were updated to include situations involving travel with laptops and tablets. Privacy training now includes visual privacy as a discussion point

Takeaway: Develop a Risk-Based Approach

- Different job functions & categories work have access to varying degrees of confidential information
- Roll out controls based on risk level
- Criteria includes
  - Level within the organization
    - C-Suite, Board of Directors, Directors, Managers
  - Sensitivity of data managed
    - PII, financial records, customer payment info
  - Time spent working outside the office
  - Frequency of travel

Takeaway: Protect Against Low-Tech Threats in Public Places

- Laptops and mobile devices are equipped with privacy filters
- Confidential documents are not reviewed in public places
- Sensitive information is not verbally discussed while on the phone or in-person
- Devices or confidential documents are not left unattended for any period of time
- Personally identifiable information is not shared verbally or displayed on a screen as it may lead to a spear phishing attack

National Retail Bank

- Business Case
  - A mock audit was conducted to determine the company's readiness to complete a full-scale compliance audit by banking regulators
    - During the audit it was discovered that the tellers' work spaces could be easily observed by co-workers and banking customers
- Solution
  - Employee communication channels used to spread results of mock audit
  - Chief Compliance Officer working to make privacy products including privacy filters mandatory at every branch: "I sleep better knowing that the use of the privacy filters is spreading throughout the branches."

Takeaway: Conduct Your Own Mock Audit

- Desk Areas:
  - Computer screens are angled away from high-traffic areas and equipped with privacy filters
  - Physical documents including company information are removed from plain view & placed in a locked drawer or box
  - Passwords not displayed on visible paper
  - USB drives removed from devices after use & put in a secure place
  - Keys, access cards and bags containing devices or company documents are not left unattended for any period of time

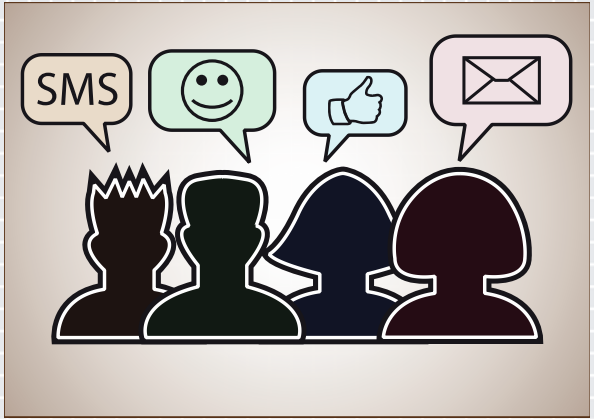
Takeaway: Conduct Your Own Mock Audit

- Copy Area
  - Documents & copies are promptly removed from printers/copiers
  - Confidential and sensitive documents are shredded
- Common Areas
  - Email and other sensitive documents are closed before projecting onto a presentation screen
  - Sensitive documents are not being reviewed in public areas, adjust physical position so that documents are angled toward a solid wall (not windows)
  - Confidential information should not be verbally discussed in common areas
  - Privacy filters used on laptops/mobile devices
  - Information is erased off of white boards following a meeting or work session

National Retail Pharmacy Chain

- Business Case
  - A main concern is the industry regulations that must be complied with, namely HIPPA and other state laws regarding the protection and handling of protected health information (PHI)
  - Working in an open retail environment raises the level of concern for low-tech threats. Customers are often in close proximity to sensitive information
  - Chief Privacy Officer, “For us, **customer trust is critical**. We are in a highly competitive and regulated industry. It is important that we demonstrate to our customers that we understand the information they are sharing is extremely personal. **Trust should be integral to our culture**.”
- Solution
  - Mandatory privacy education trainings for all clinical employees and management, focus is on communicating policies and procedures for data protection coupled with tools like privacy filters on kiosks

Takeaway: How to Create an Effective Data Security Communication Plan



- Target Your Audiences
- Provide Ongoing Education
- Make it Personal & Relatable
- Encourage a Cultural Change
- Equip employees with a Data Privacy/ Security Toolkit
- **Remember:** Data security is not one size fits all, nor is a data security communication plan

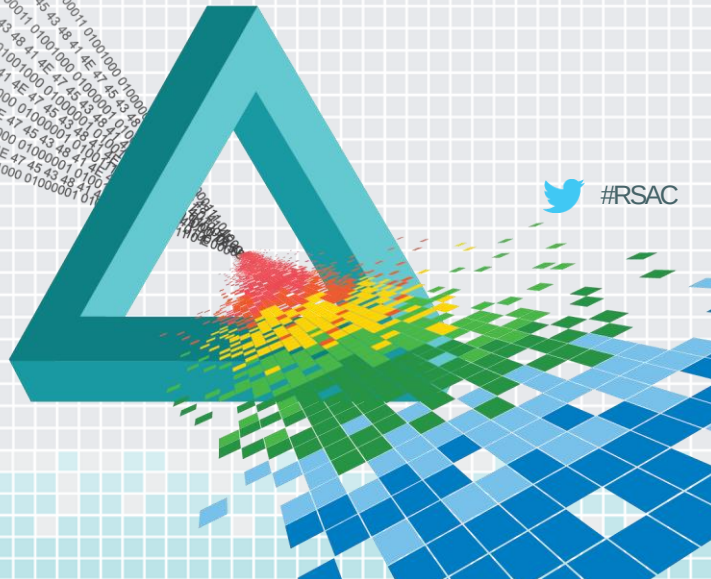
Takeaway: Creating your Data Privacy / Security Toolkit

- Layer physical and software security technologies for a defense-in-depth approach
- Equip newly-issued devices with pre-installed security technologies
  - Could include privacy filters, encryption software, IAM, remote wipe capabilities, physical locks
- Require masked passwords on devices
- Provide secure storage for sensitive documents and enact a clean desk policy
- Equip copy rooms with shredders to dispose of confidential documents

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Creating a Visual Privacy Standard



#RSAC

Where Visual Privacy Standards Fit Within the Larger Data Security Policy

- This standard may fall under any number of security and privacy policy sections depending on how your company structures the IT Security plan, including but not limited to:
  - Identity and Access Management Policy
  - Privacy Policy
  - Compliance Policy

Component 1: Worker Adherence

- Use this section to clearly outline the functions and levels of workers that should adhere to the standard.
  - **Example:** All company workers (employee, contingent/contract workers, and temporary staff) who fit the following criteria of being at high risk for visual hacking.
    - Business travelers (flying, commuting on public transit, etc.)
    - Those who frequently access company information that is confidential or regulated. This type of information could include but is not limited to Financial, HR, Customer Data, Trade Secret, etc. Special attention should be paid to situations where office floor plans are open and walk-by visual access is common
    - Those who regularly spend time working outside the office (accessing email and texts or working on company confidential documents)
    - Those in leadership roles within the company

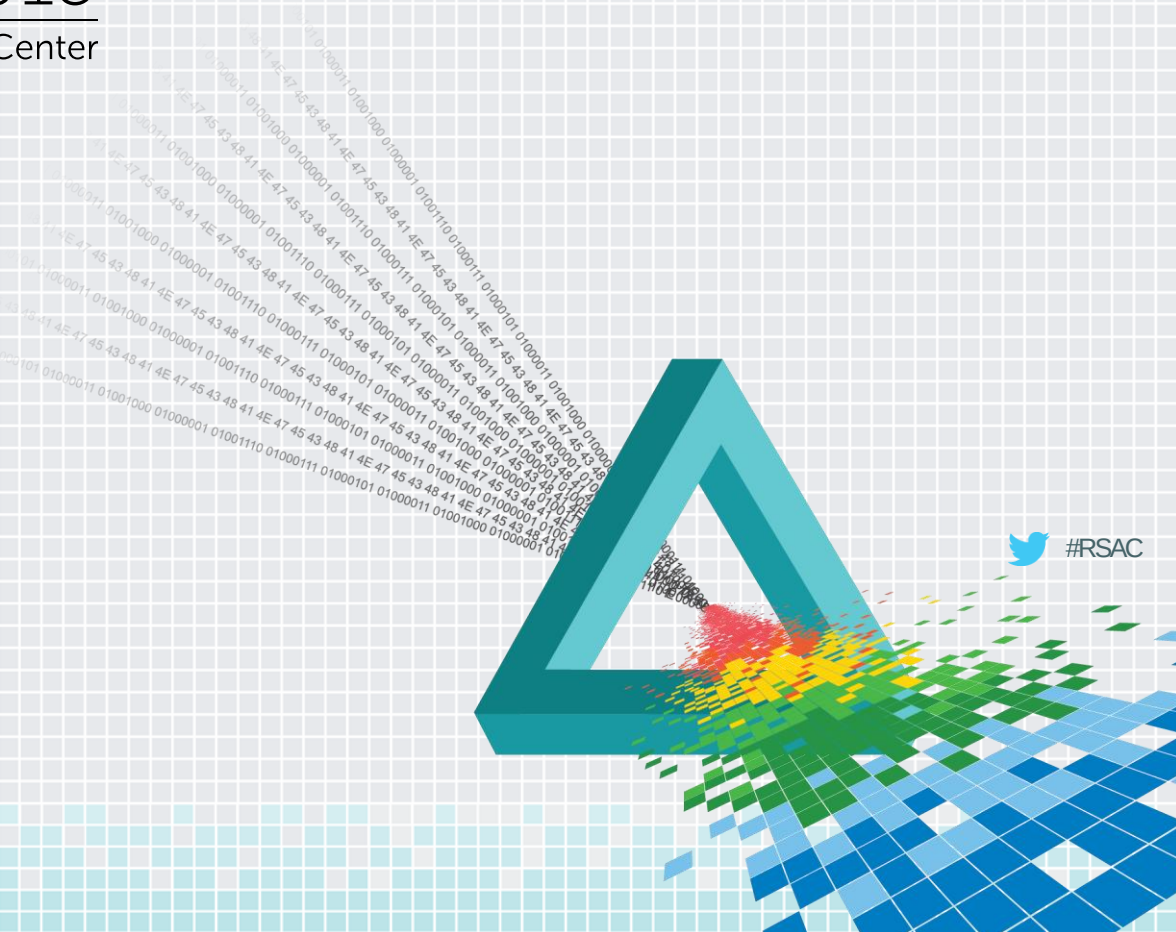
Component 2: Standard Statement

- Use this section to outline how and where company workers should use tools like privacy filter (desktop and laptop computers) and privacy screen protector (smartphone and tablets) products, password masking etc.
  - Example: Use privacy filters and privacy screen protector products and password masking to help protect company information from unauthorized views:
    - On all in-office devices used by at-risk employees that have a high risk for walk-by visual hacking
    - On all devices used to access company information in public areas
    - On all devices used by employees when working outside the office, including home or remote office

Component 3: Related Information

- Use this section to refer workers to additional resources on the topic of Visual Privacy. Link to relevant policies, best practices and other resources to give employees a holistic view of company security measures
  - Example: For additional information regarding visual privacy and visual hacking, please see the following resources:
    - Link to Relevant Policies
    - Link to Visual Privacy Best Practices
    - Privacy Filter and Screen Protector Product Page Link

Best Practices



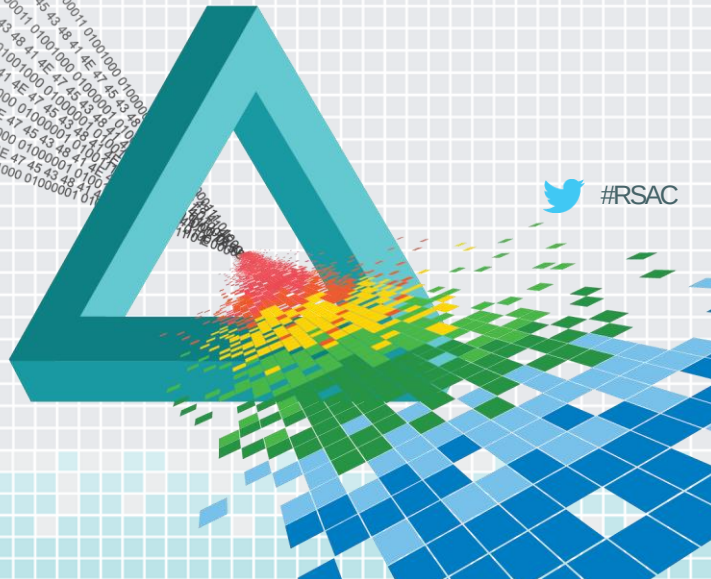
A Review of Best Practices for IT Security Teams

- Ensure that IT security plans include language on low-tech threats like visual privacy and visual hacking
- Educate employees on the risks posed by low-tech threats
- Identify those employees within the organization most at risk for visual hacking
- Equip all workers, especially those deemed “at risk,” with a “Data Privacy/Security Toolkit” that offers resources to aid in combatting visual hacking
- Proactively complete routine situation and site analyses to use as awareness tools

Best Practices for Company Employees

- Utilize your Data Privacy/Security toolkit
- Secure your workspace
- Analyze your surroundings
- Become a data privacy and security champion
- Make it a priority to attend ongoing education offerings

Summary & Next Steps



Summary

- It's easy to get caught up in the "flavor of the week" of privacy and security measures – don't forget the basics & low-tech threats
- Equipping workers with tools like privacy filters & password masking, which can help mitigate the human factor, should be coupled with ongoing education and communication efforts to maximize impact
- Encouraging a culture within the office where data privacy and security are held in the highest regard will be important moving forward as hacks will only continue to grow in number and impact

Apply: Where to Go From Here

- Next week you should:
  - Review your company's policies and standards to determine if they address low-tech threats like visual hacking
- In the first three months following this presentation you should:
  - Complete a mock audit to identify vulnerabilities within the organization for low-tech threats
  - Categorize employees into risk groups for visual hacking attacks and begin to roll out controls to those deemed most "at risk"
  - Begin including low-tech threats in ongoing data privacy & security education and communication efforts

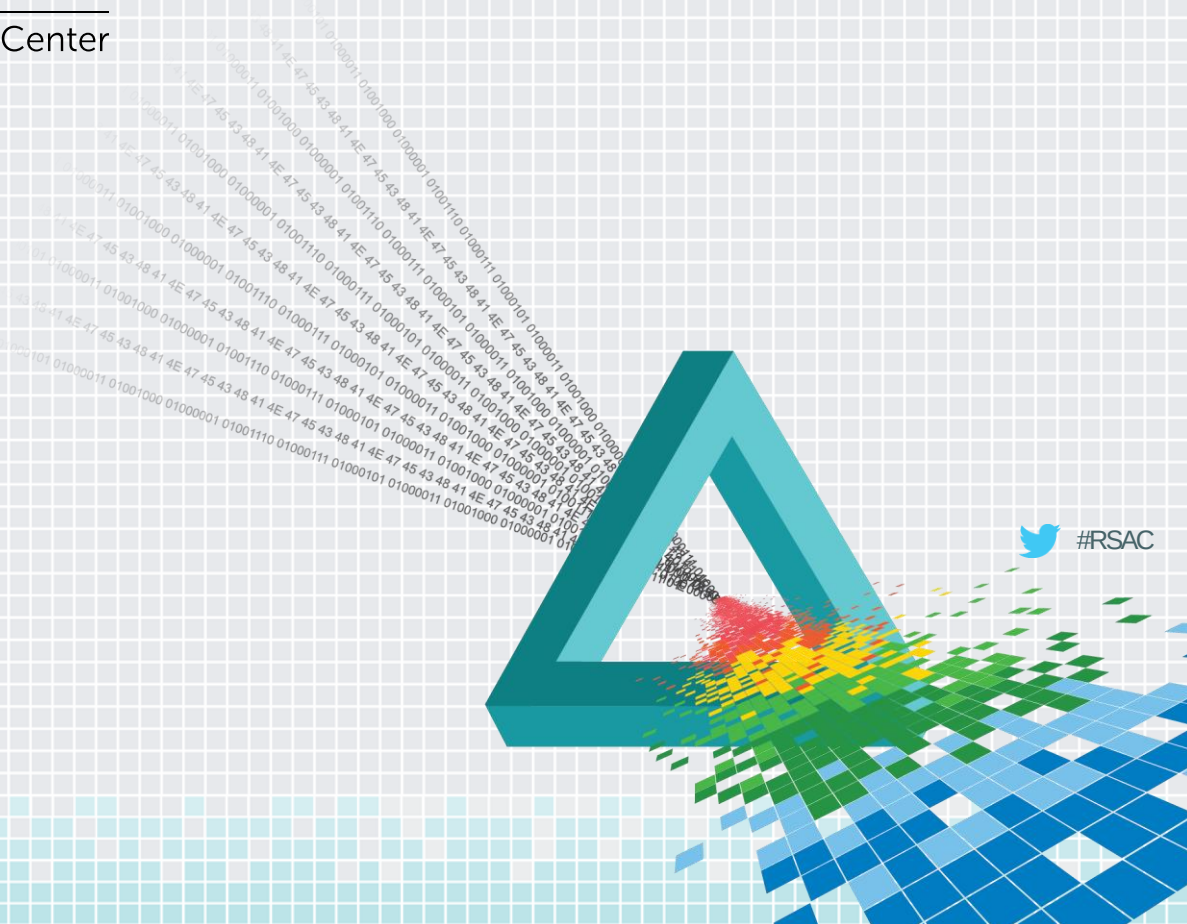
Apply: Where to Go From Here

- Within six months you should:
  - Ensure that a Visual Privacy Standard has been adopted, if not addressed in current policies
  - Continue communication and education efforts on low-tech threats
  - Work to protect against low-tech threats by including tools to combat them with each device issued to the workforce and for BYOD devices, make sure certain measures are met
    - For physical documents, lock boxes and shredders should be readily available

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Questions?



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!