CUNA
Technology
COUNCIL

Top Security Challenges Facing Credit Unions Today

Chris Gates

Lares Consulting

24 September 2013

A Little About Me…

Chris Gates

Employment History:

- Partner, Lares
- Senior Security Consultant-Rapid7
- Network Attack Team Lead-Applied Security Inc.
- Penetration Tester-Booz Allen Hamilton
- Computer Exploitation Technician-US Army Red Team
- Signal Officer-US Army

- Professional Certifications:
  - CISSP
  - CISA
  - SANS GCIH, GPEN
  - CEH
- Security Stuff:
  - Member of Metasploit Project
  - Contributor to Ethical Hacker.net
  - Active security blogger/twitter/community/Infosec Mentors
  - Penetration Testing Execution Standard Core Member (PTES)

Chris

carnal0wnage.attackresearch.com

@carnal0wnage

Previous Talks

- Evolution of Pentesting High Security Environments
- ColdFusion for Pentesters
- From LOW to PWNED
- Information Operations for MGMT
- Dirty Little Secrets(pt 1/pt 2)
- Attacking Oracle (via TNS & web)
- Open Source Information Gathering
- Client-Side Attacks

Blog Archive

- ▶ 2013 (14)
- ▶ 2012 (53)
- ▶ 2011 (50)
- ▶ 2010 (54)
- ▶ 2009 (125)
- ▶ 2008 (169)
- ▶ 2007 (73)

Who Is Lares?

- Minimum of 10 years Infosec Experience per consultant (35+ combined)
- Penetration Testing Execution Standard Core Members
- Publications
  - Aggressive Network Self Defense
  - Contributing writer to COBIT
  - Contributing writer to ISO17799, and one of less than 1000 certified auditors of the ISO17799 (international standards for security best practices)
  - Author of multiple national / international security awareness training programs
- Speaking Engagements all over the world

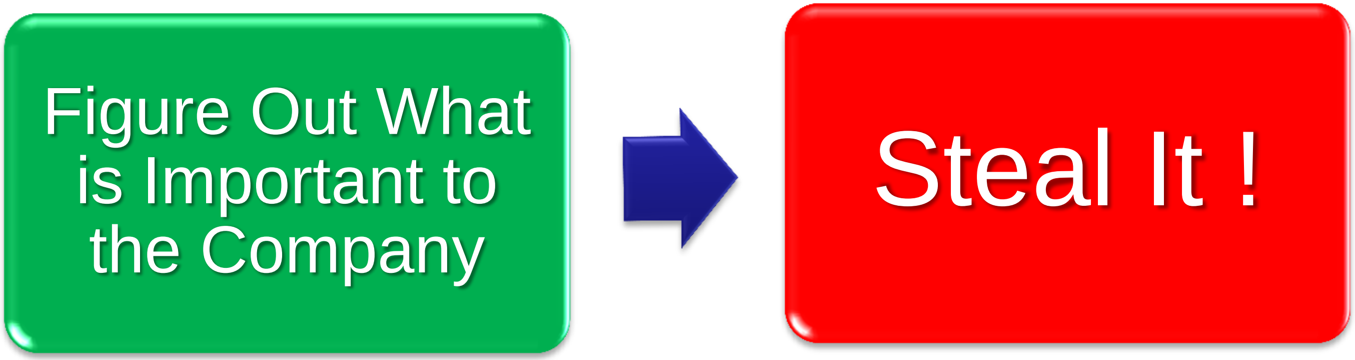


Figure Out What is Important to the Company

Steal It !

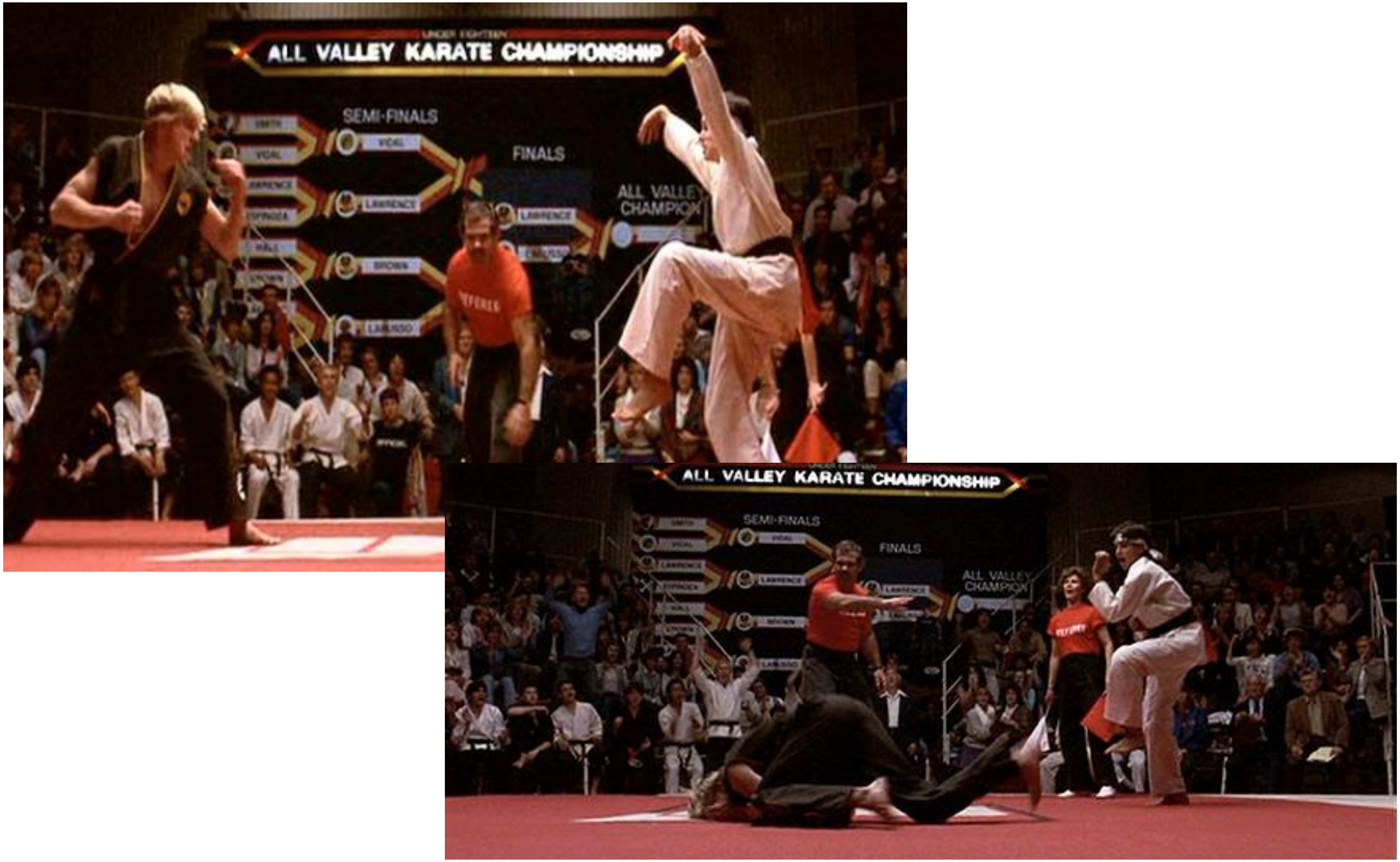
TOP THREATS FACING YOUR ENTERPRISE

Karate Kid Ruined Us!

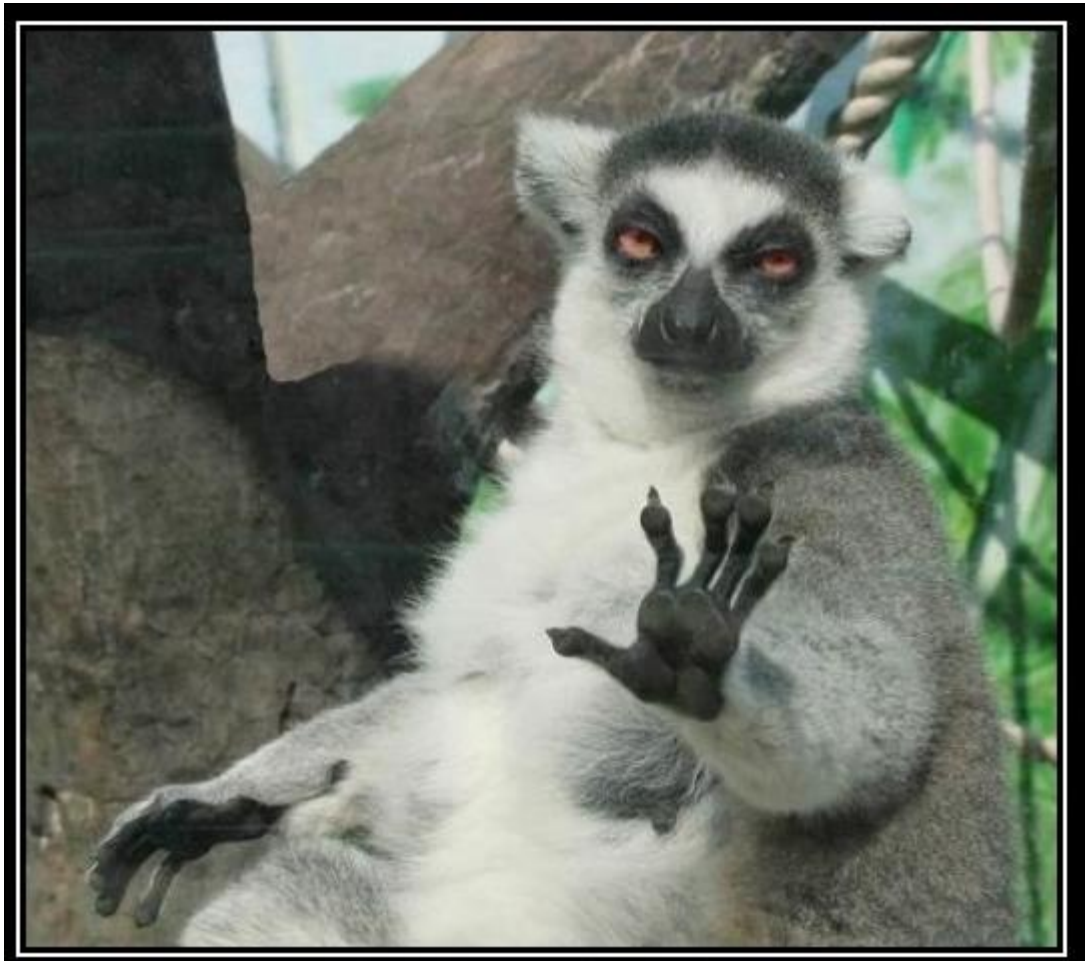
Shouts to Haroon Meer: http://repo.staticsafe.ca/presentations/hitbsecconf2012/D1T2%20-%20Haroon%20Meer%20-%20You%20and%20Your%20Research.pdf

Karate Kid Ruined Us!

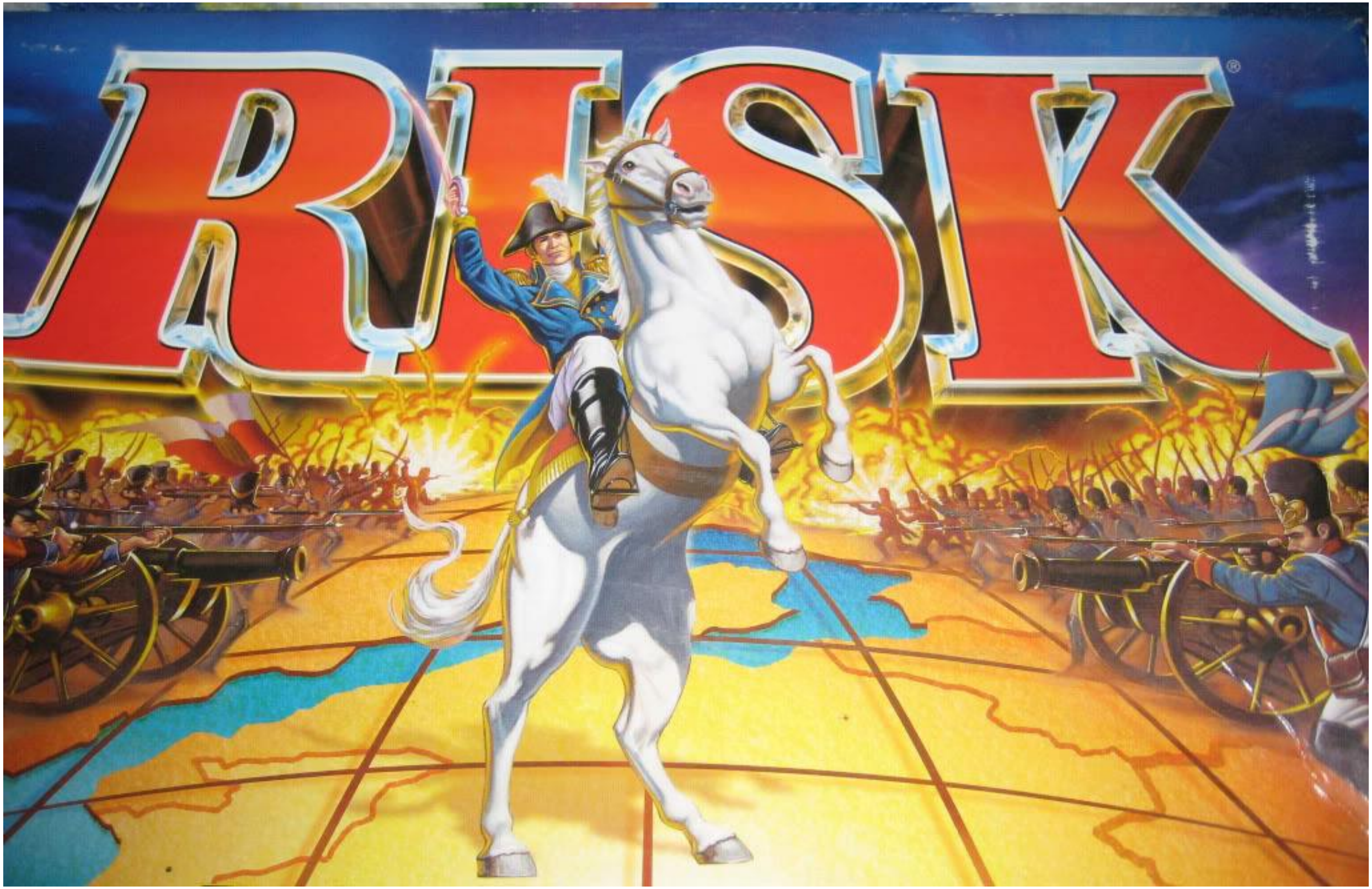
Karate Kid Ruined Us!



Karate Kid Ruined Us!



Having No Security Policies

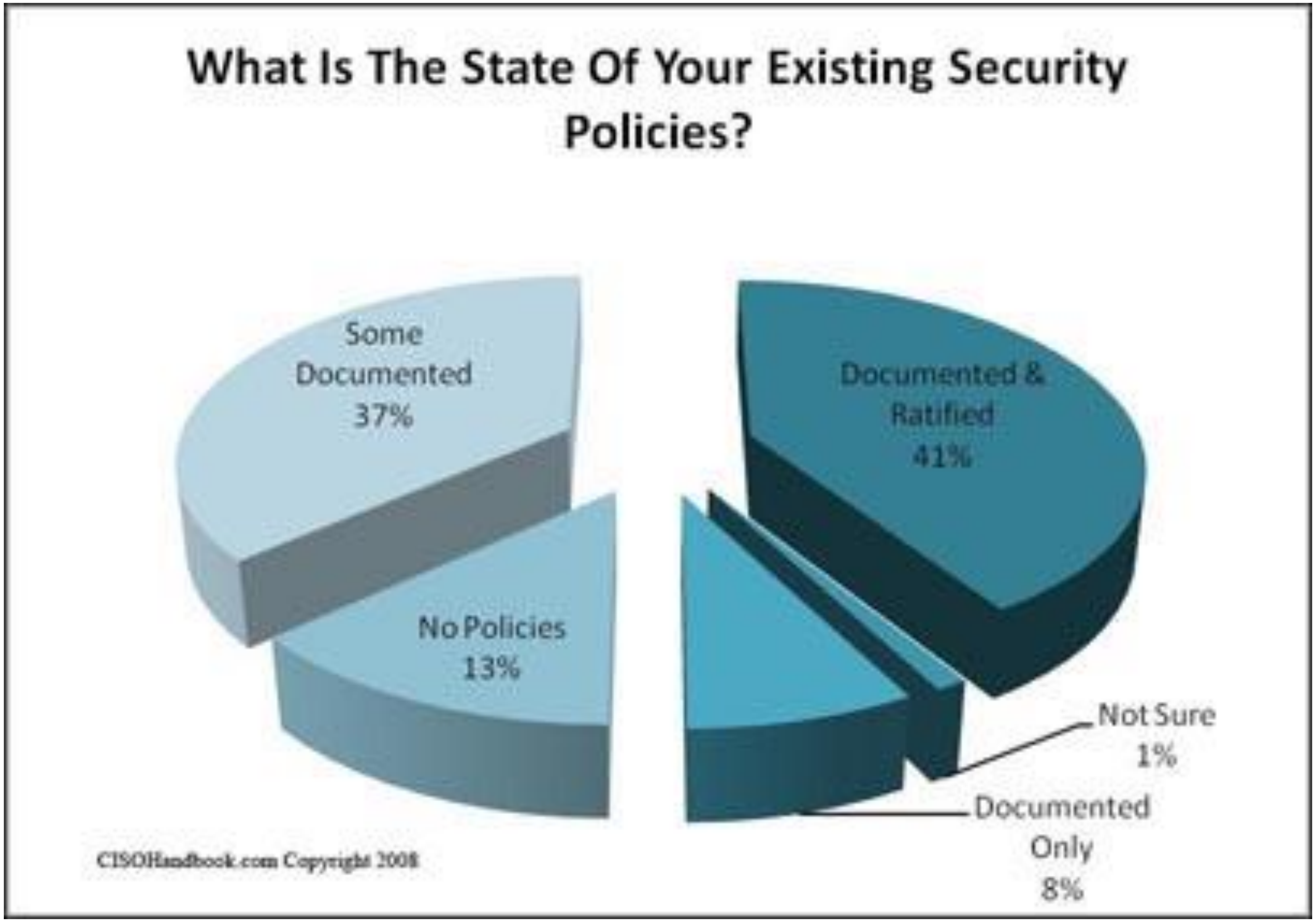


Having No Security Policies

- All security testing is based on YOUR adherence to YOUR security policies

- If you have none, what are you testing?

Having No Security Policies



Having No Security Policies

- For this audience you most likely have policies due to compliance reasons.

- Do they document what you actually do? Or did you download them from the internet and change the logo?

- How do we test your policies?
  - – Risk Assessments (design)
  - – Penetration Tests (effectiveness)

Risk Assessment

- Performing Risk Assessments is the single best way to get a snapshot of the state of your policies.

- You can then begin testing the EFFECTIVENESS of your policies via security testing

What is a Risk Assessment?

“Information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. In its simplest form, a risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks.”

http://laresconsulting.com/risk.php

AUDITING

What my friends think I do

What my mom thinks I do

What society thinks I do

What the partners think I do

What I think I do

What I actually do

Risk Assessment

Reasons to Conduct

- Compliance with regulations
- Overall health check of the InfoSec program
- Gain understanding of program Effectiveness
- Baseline discovery
- To show 3rd parties and customers they are “Secure”

How it’s usually done

- Whip out a checklist
- Check stuff off on checklist
- Have a TON of interviews
- Believe every word
- Do a tick mark legend and ask people to provide “evidence” *which is usually biased*
- Only assess controls that are in scope of THAT specific assessment *often information centric*

Setting a Risk Assessment Up to Fail

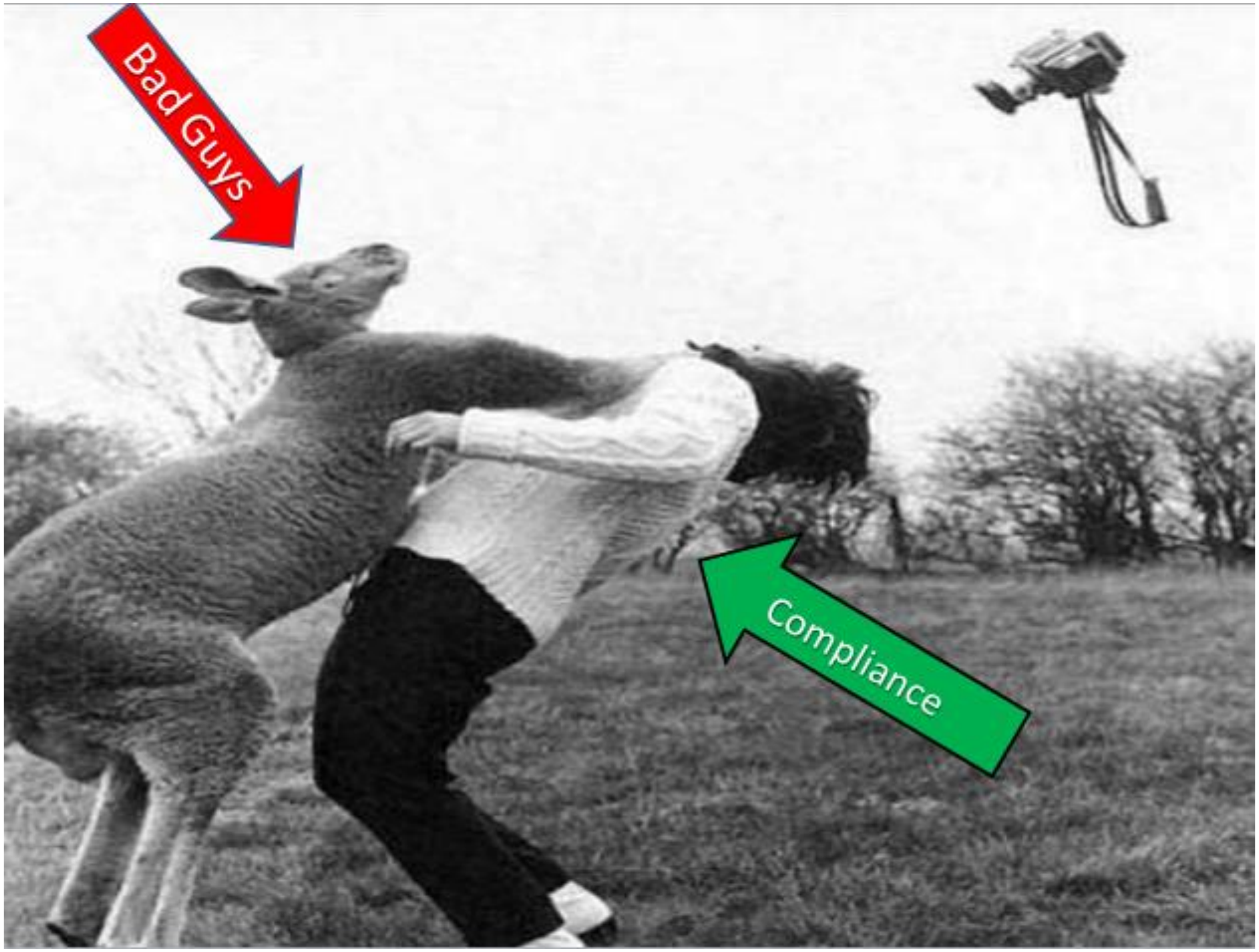
- Do not allow ACTUAL/TECHNICAL testing and validation
- Rely on all information provided as TRUE
- Minimize scope to only include assets and controls that are part of the selected compliance regulation and NOT the ENTIRE BUSINESS
- Allow for “Compensating Controls” to be an answer to most issues
- Expect to become compliant through outsourcing
- Expect to become compliant through product purchase/implementation
- Business “accepts the risk” and accepts forever
- Be unprepared
- LIE

Compliance Vs. Security

- Compliance audits are designed to capture the state of an org at a point in time
- Security requires constant interaction between management, the business and the assets
- Example: PCI Compliance Assessments
  - Only focuses on “card holder” environment
  - (De)Scoping increases your risk and impacts accuracy of risk measurement
- Compliance allows you to legally operate the business
- Security provides you peace of mind knowing your business can sustain a real attack

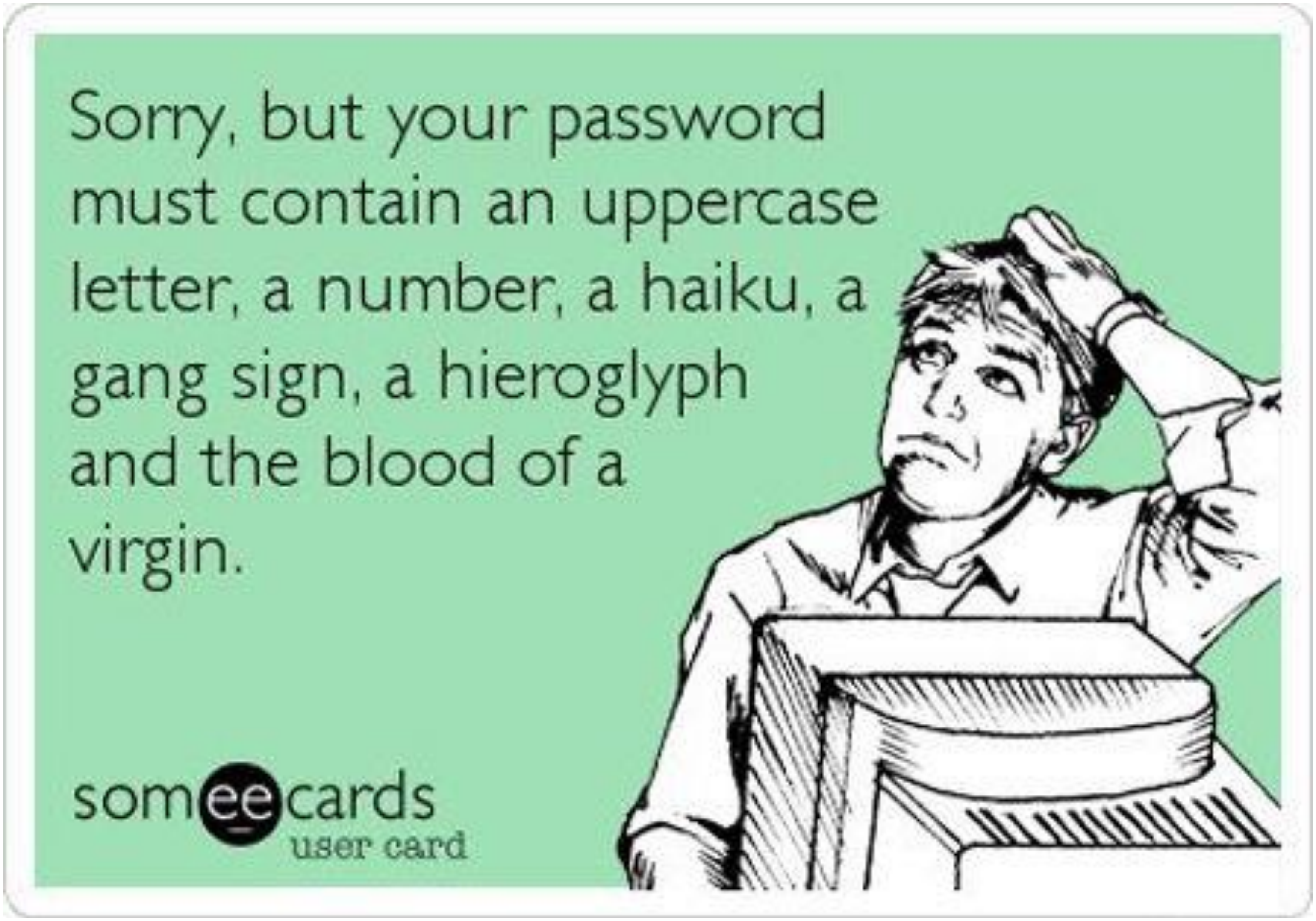
CUNA Technology COUNCIL

Compliance Vs. bad Guys



Self Assessments

Passwords



Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.

Passwords

- In general people’s passwords and password policy are horrible.

- Passwords recently used to compromise organizations:

-kiosk/kiosk

-besadmin/blackberry

-$username/Company1

-mailman/mailman

-$username/Password1

-$username/password <-!!!

Setting Password Policies Up to Fail

- Not educating users on creating good passwords
- Not regularly auditing passwords
- Not regularly auditing/rotating default/service accounts
- Weak Password GPO because users “cant remember longer passwords”
- Adding administrative privileges to user accounts instead of separate admin accounts (joeuser is domain admin instead of joeuser-admin)
- Static local admin passwords

Remote Access

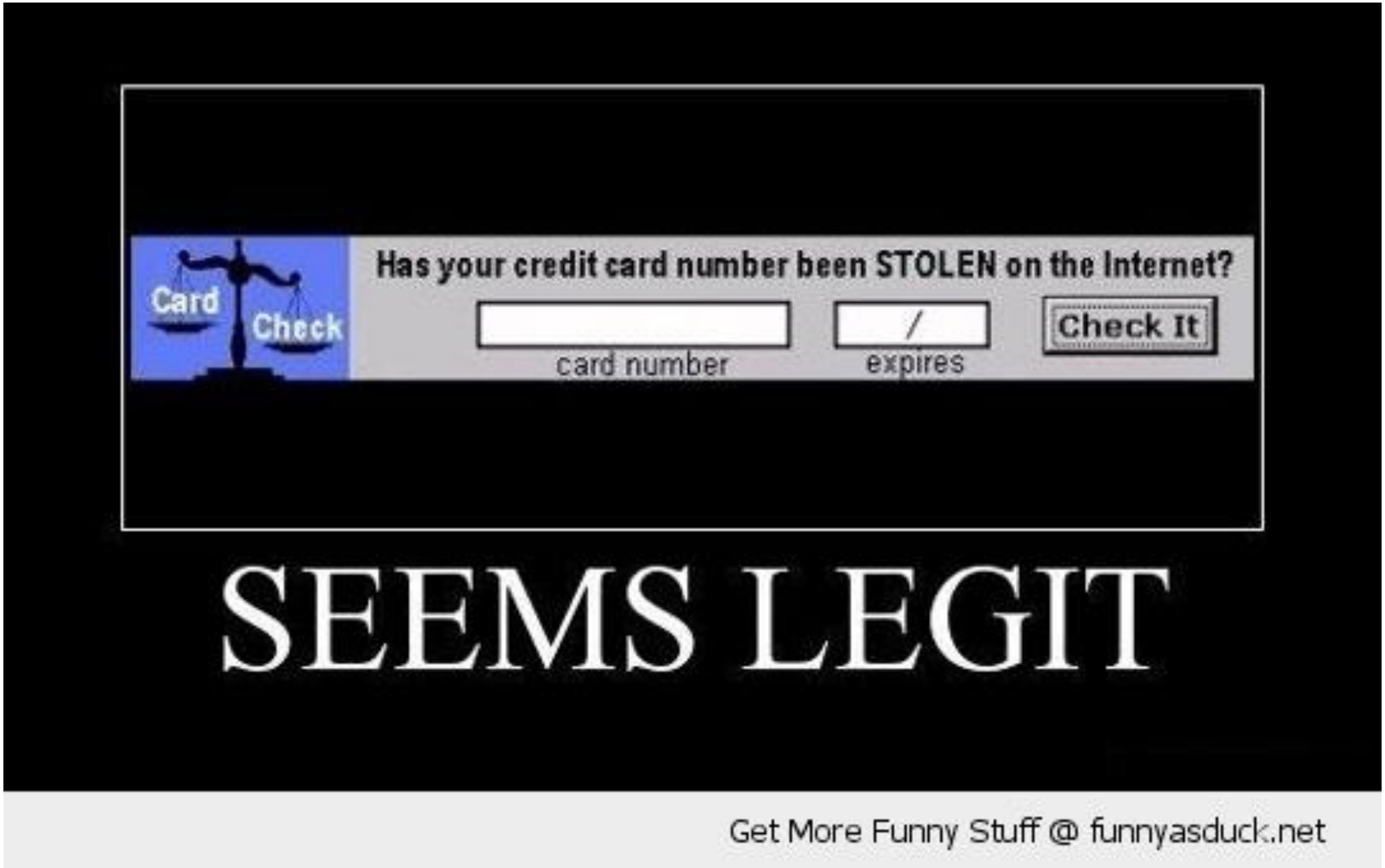
Remote Access

- Single Factor webmail solutions
  - – OWA, Squirrelmail, etc
  - – Grab address book, repeat brute forcing
  - – Search public folders
  - – Search for (default) passwords
- Single Factor VPN solutions
  - – Cisco SSL VPN, Juniper SSL VPN, Citrix
  - – Typically puts you right on the internal network with no restrictions

Setting Remote Access Up to Fail

- Not putting everything behind the VPN (OWA)
- Single Factor
- Not monitoring/configuring allowed users/groups
- Not segmenting VPN access from rest of network
- No Citrix Hardening
- Multiple Remote Access Solutions

People Clicking Stuff



Has your credit card number been STOLEN on the Internet?

Get More Funny Stuff @ funnyasduck.net

People Clicking Stuff

- It happens…
- Education vs. Technical Controls
- Spam Gateways
- Web Proxies
- Workstation Baselines

People Clicking Stuff

- How to Test/Train?
- Social Engineering Assessments
  - Start with obvious work your way up to targeted attacks
- Turn Phish spotting into a game
  - Reward first employee to spot/report a phish with a gift card.

Setting Social Engineering Testing Up to Fail

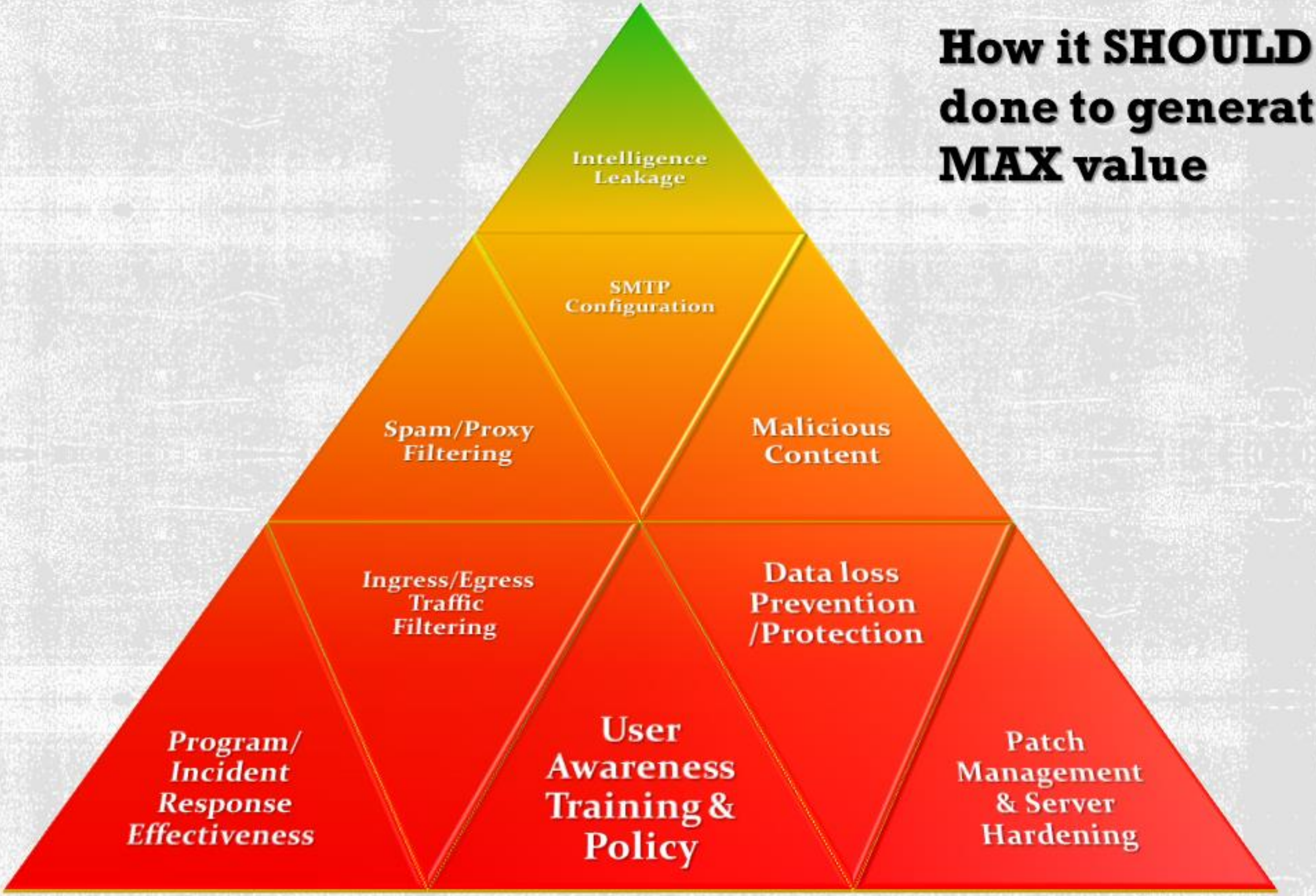
Common Misconceptions

- We will get owned, what's the point
- It will offend our users
- Doesn’t provide enough value

How its usually done

- Send a 419 scam style email
- Track clicks
- Write a report to show who clicked

How it SHOULD be done to generate MAX value


Intelligence Leakage
SMTP Configuration
Spam/Proxy Filtering
Malicious Content
Ingress/Egress Traffic Filtering
Data loss Prevention /Protection
Program/ Incident Response Effectiveness
User Awareness Training & Policy
Patch Management & Server Hardening

Ingress/Egress Filtering

Ingress/Egress Filtering

- Usually not that good
  - Relying on router ACLs or network proxies
  - Default settings
- No Email = No Problem

Setting Ingress/Egress Filtering Up to Fail

- Not exhaustively testing outbound ports protocols
- WCCP
- Open web proxy policy
  - Not blocking uncategorized sites
- Critical servers can talk to the Internet

Patching/Workstation/Server Hardening

- Patching
  - Windows usually handled, 3rd party not so much
- Secure Deployment Builds
  - Workstations and Servers
  - Create them, update them, use them
- NIST, NSA, Vendor
  - NIST: http://web.nvd.nist.gov/view/ncp/repository
  - NSA: http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

Setting Patching/Workstation/Server Hardening up to Fail

- Not doing any of it
- No “gold” image
- No credentialed scanning
- No 3rd Party Patching
- Waiting for an email to tell you something is wrong

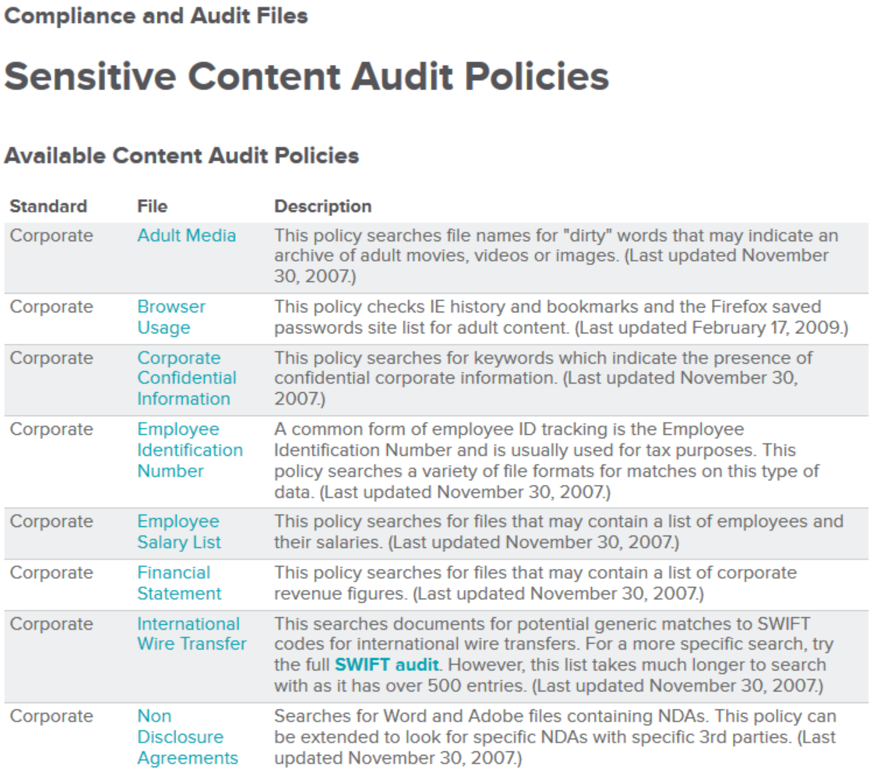
Internal Visibility

Internal Visibility

Know Where Your Sensitive Data is and Protect It

Know Where Your Sensitive Data is and Protect It

- DLP Solutions /OpenDLP
- Scan for it with scripts or vulnerability scanners



Compliance and Audit Files

Sensitive Content Audit Policies

Available Content Audit Policies

Standard	File	Description
Corporate	Adult Media	This policy searches file names for "dirty" words that may indicate an archive of adult movies, videos or images. (Last updated November 30, 2007.)
Corporate	Browser Usage	This policy checks IE history and bookmarks and the Firefox saved passwords site list for adult content. (Last updated February 17, 2009.)
Corporate	Corporate Confidential Information	This policy searches for keywords which indicate the presence of confidential corporate information. (Last updated November 30, 2007.)
Corporate	Employee Identification Number	A common form of employee ID tracking is the Employee Identification Number and is usually used for tax purposes. This policy searches a variety of file formats for matches on this type of data. (Last updated November 30, 2007.)
Corporate	Employee Salary List	This policy searches for files that may contain a list of employees and their salaries. (Last updated November 30, 2007.)
Corporate	Financial Statement	This policy searches for files that may contain a list of corporate revenue figures. (Last updated November 30, 2007.)
Corporate	International Wire Transfer	This searches documents for potential generic matches to SWIFT codes for international wire transfers. For a more specific search, try the full **SWIFT audit**. However, this list takes much longer to search with as it has over 500 entries. (Last updated November 30, 2007.)
Corporate	Non Disclosure Agreements	Searches for Word and Adobe files containing NDAs. This policy can be extended to look for specific NDAs with specific 3rd parties. (Last updated November 30, 2007.)

How to Test the Previous Slides

- Vulnerability Assessments

- Penetration Testing

Vulnerability Assessments

- **A vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
  - http://en.wikipedia.org/wiki/Vulnerability_assessment

Vulnerability Assessments

Reasons to Conduct

- Identify potential vulnerabilities
- Provide scoring of risk & prioritization of remediation
- Manage environment vulnerabilities over time to show security program improvement, defense capability increase and compliance with ongoing patch, system and vulnerability lifecycle

How it’s usually done

- Run a bunch of scanners
- Generate a report
- **Sometimes** Generate a custom report consisting of copy/paste data from the Vulnerability scanners and TRY to make sure you delete the word Nessus, qualys… and/or the previous clients name

Setting Vulnerability Assessments Up to Fail

- Do not run “Dangerous or Experimental Checks” *instant 30%+ reduction in results and overall accuracy*
- Do not run thorough checks
- Do not run Web checks
- Limit IP/Ports to scan
- Only run ONE brand of scanner
- Limit only to known network checks
- Only scan once

Penetration Testing

- A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source... The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.
  - http://en.wikipedia.org/wiki/Penetration_test

HACKER

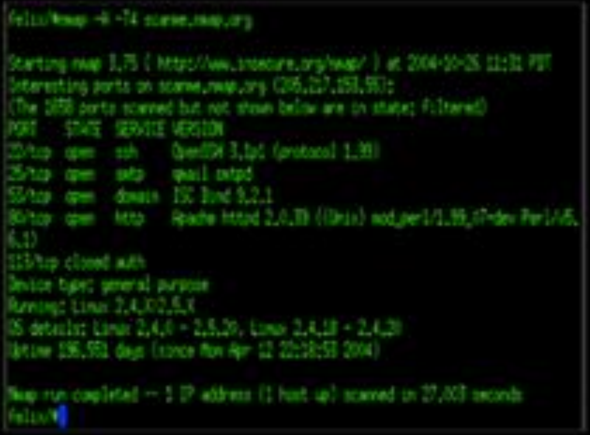
What my friends think I do

What my Mom thinks I do

What society thinks I do

What the government thinks I do

What I think I do



```
felix/# nmap -A -T4 scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2004-10-25 11:31 PDT
Interesting ports on scanme.nmap.org (205.217.153.53):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp  open   smtp    qmail smtpd
53/tcp  open   domain  ISC Bind 9.2.1
80/tcp  open   http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.
6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 156.551 days (since Mon Apr 12 22:18:53 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 27.003 seconds
felix/#
```

What I actually do

Penetration Testing

Reasons to Conduct

- Identify if attackers can readily compromise the security of the business
- Identify potential impact to the business
- Confirm vulnerabilities identified
- Gain a “Real World” View of an attackers ability to “hack” the environment and resolve issues identified

How it’s usually done

- Do all the steps in Vulnerability Assessment listed previously
- Run metasploit/Core/Canvas against hosts
- Try a few other automated tools
- Call it “SECURE” If those don’t work

Setting Penetration Testing Up to Fail

- Do not allow the exploitation of systems
- Restrict testing to non production systems
- Restrict the hours of testing
- Restrict the length of testing
- Improperly scope / fail to include ALL addresses
- Only perform externally
- Patch/fix BEFORE the test
- Only allow directed attacks (no SE/ Phishing)
- Lack of focus on BUSINESS risk and increased focus on technical issue
- Not impact or goal oriented

Distributed Denial Of Service (DDOS)

- Mostly Solved
  - – Pay for protection.
  - – Akamai, Prolexic, cloudfare, etc

Web Applications/Mobile Applications

Have to pick the right test for the right job

Web Applications/Mobile Applications

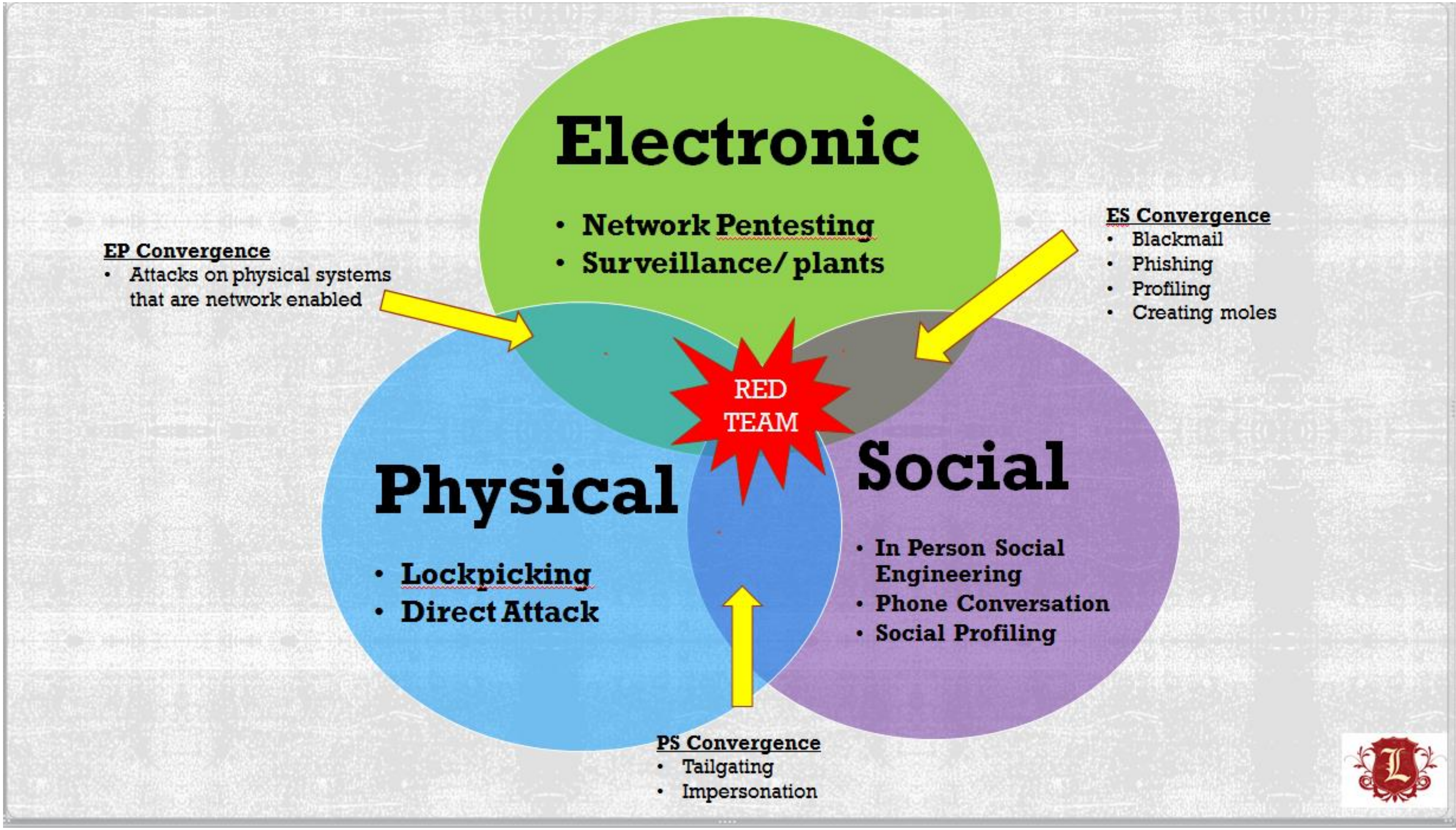
- Mostly solved
  - Just have to put in the effort/pay for the assessments
- Outsourced vs. In House
- In-House
  - SDLC & Security Testing
  - Your RA should tell you how this is doing ☺
- Outsourced
  - Security reviews in contracts
  - Require vendor to perform testing prior to deployment (on their $$)

Red Team Testing

The term originated within the military to describe a team whose purpose is to penetrate security of "friendly" installations, and thus test their security measures. The members are professionals who install evidence of their success, e.g. leave cardboard signs saying "bomb" in critical defense installations, hand-lettered notes saying that “your codebooks have been stolen" (they usually have not been) inside safes, etc. Sometimes, after a successful penetration, a high-ranking security person will show up later for a "security review," and "find" the evidence. Afterward, the term became popular in the computer industry, where the security of computer systems is often tested by tiger teams.

How do you know you can put up a fight if you have never taken a punch?

Red Team Testing



Electronic

- Network Pentesting
- Surveillance/ plants

Physical

- Lockpicking
- Direct Attack

Social

- In Person Social Engineering
- Phone Conversation
- Social Profiling

RED TEAM

EP Convergence

- Attacks on physical systems that are network enabled

ES Convergence

- Blackmail
- Phishing
- Profiling
- Creating moles

PS Convergence

- Tailgating
- Impersonation

Red Team Testing

Reasons to Conduct

- Real world test to see how you will hold up against a highly skilled, motivated and funded attacker
- The only type of testing that will cover a fully converged attack surface
- Impact assessment is IMMEDIATE and built to show a maximum damage event
- This IS the FULL DR test of an InfoSec Program

Questions?

Thank You!

Chris Gates

cgates@laresconsulting.com

www.lares.com