COMPLIANCE

The ASSAULT ON REASON

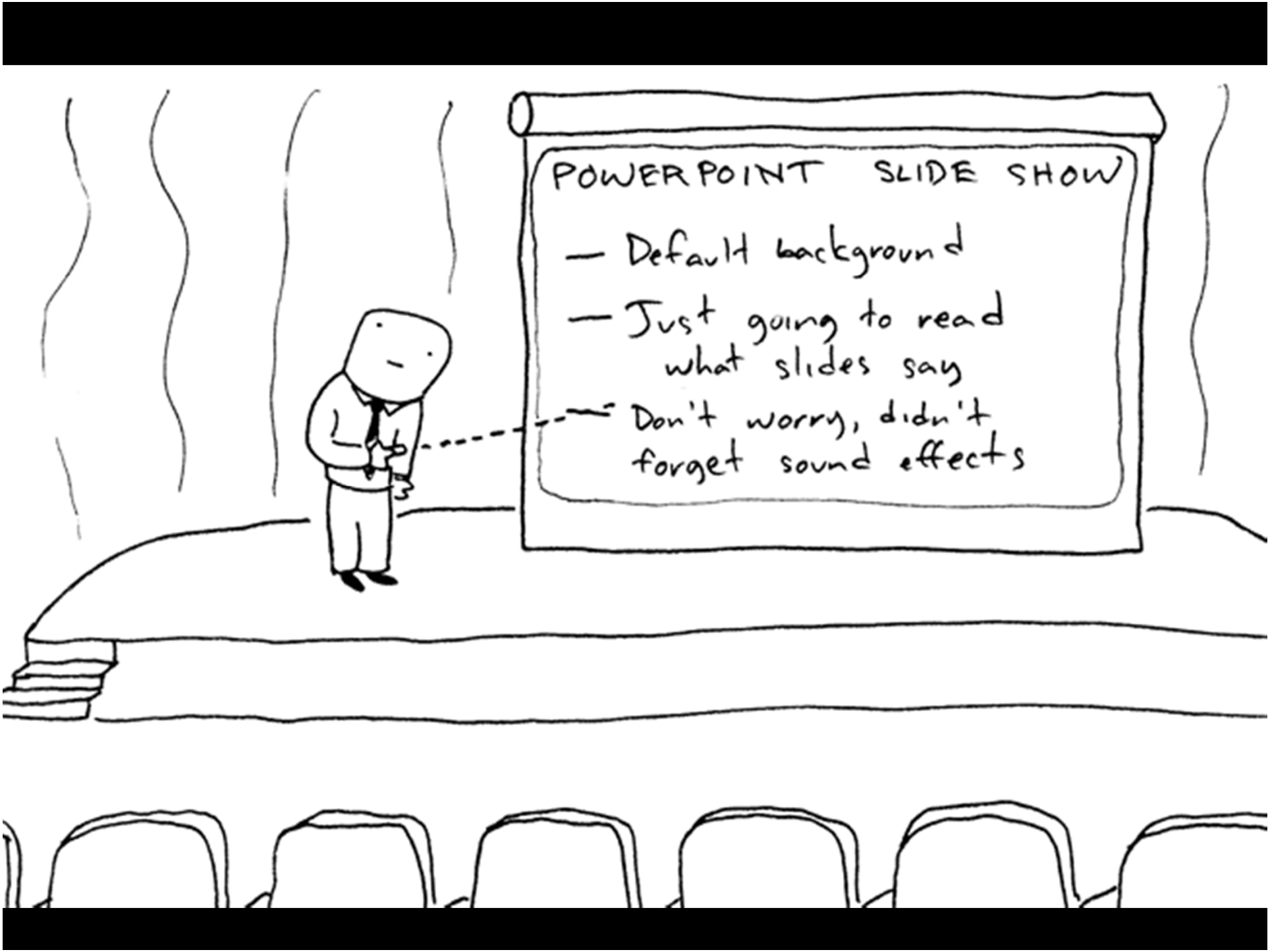
CHRIS NICKERSON

hi. =)

Thanks

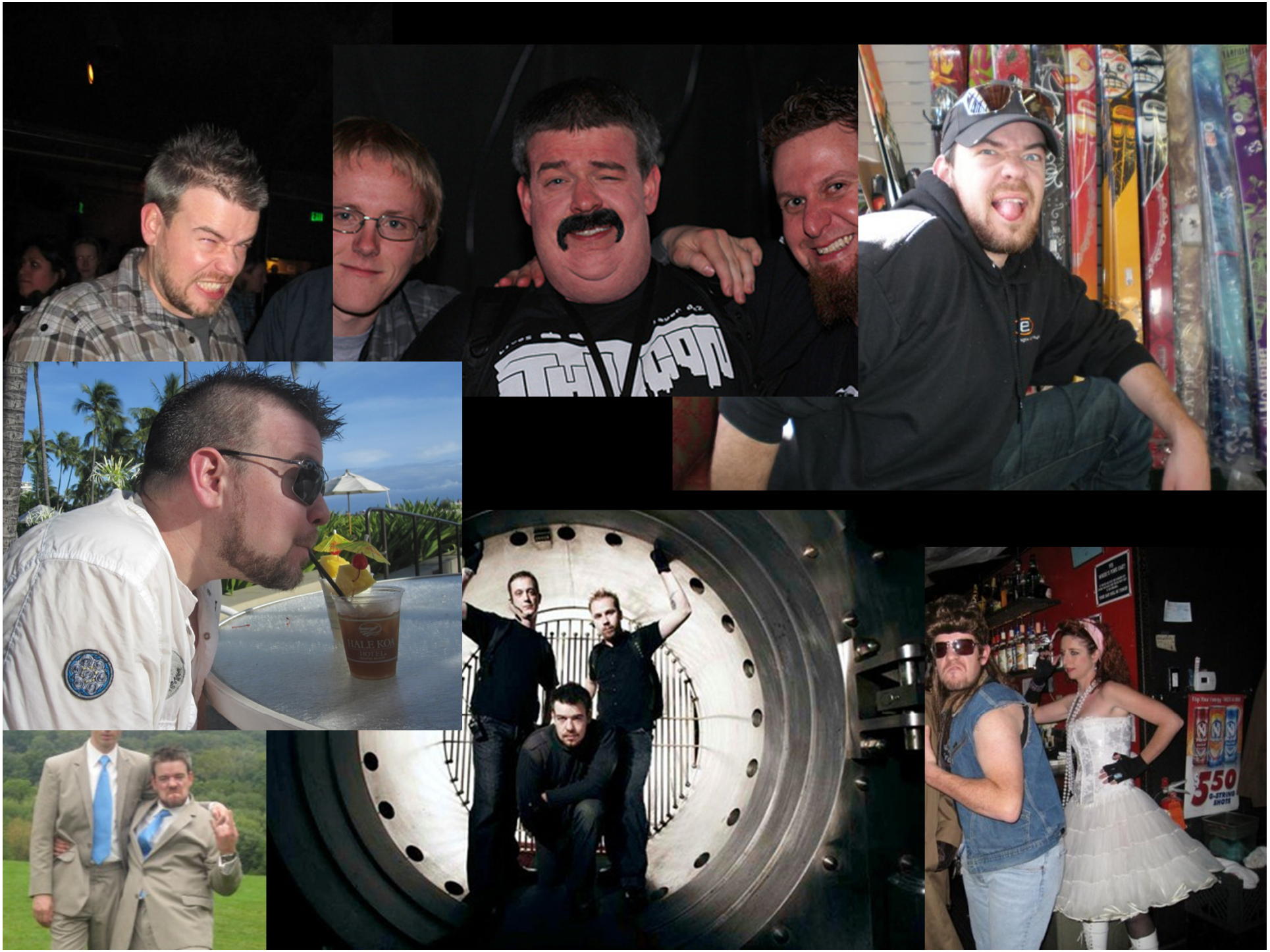

Colombia
International boundary
Internal administrative boundary
National capital
Internal administrative capital
Railroad
Road
Caribbean Sea
North Pacific Ocean
NETHERLANDS ANTILLES
VENEZUELA
PANAMA
ECUADOR
PERU
BRAZIL
ARAUCA
CASANARE
VICHADA
META
GUAINÍA
GUAVIARE
CAQUETÁ
VAUPÉS
PUTUMAYO
AMAZONAS
Bogotá
Boundary representation is not necessarily authoritative.

And.....

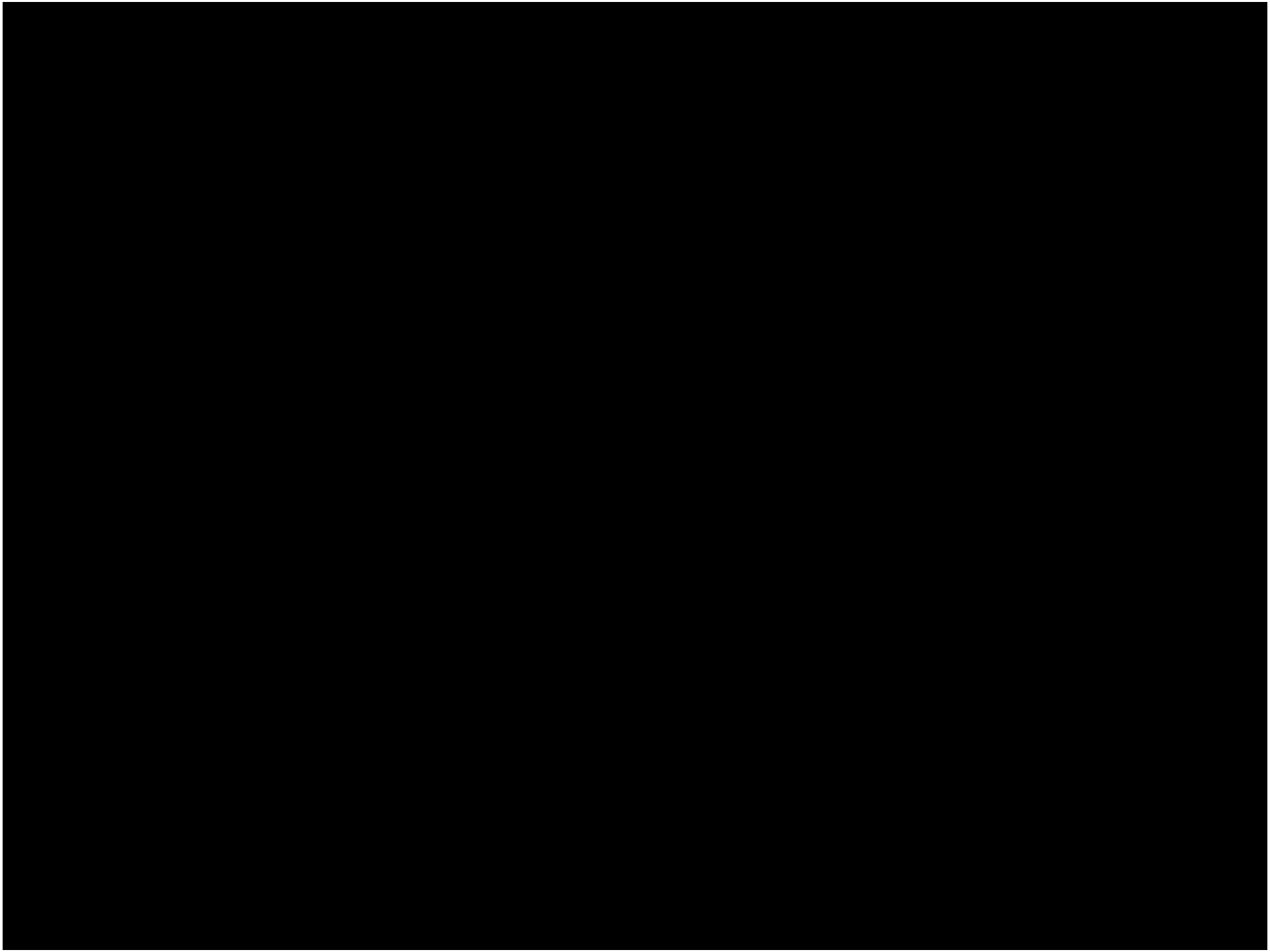

POWERPOINT SLIDE SHOW
— Default background
— Just going to read what slides say
— Don't worry, didn't forget sound effects

Anyway...

I’m Chris



My Credentials?



- Pain in the arse
- Loudmouth
- Security Punk
- Tells lies (professionally)
- Is called all sorts of bad words.. That I will likely say throughout this talk
- Cant code well
- Talks $hit
- Drinks a LOT
- Is an overall J3rk

-me

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION®

hereby certifies that

Willem A. Fourie

has successfully met all requirements and is qualified as a

Certified Information Systems Auditor

CISA®

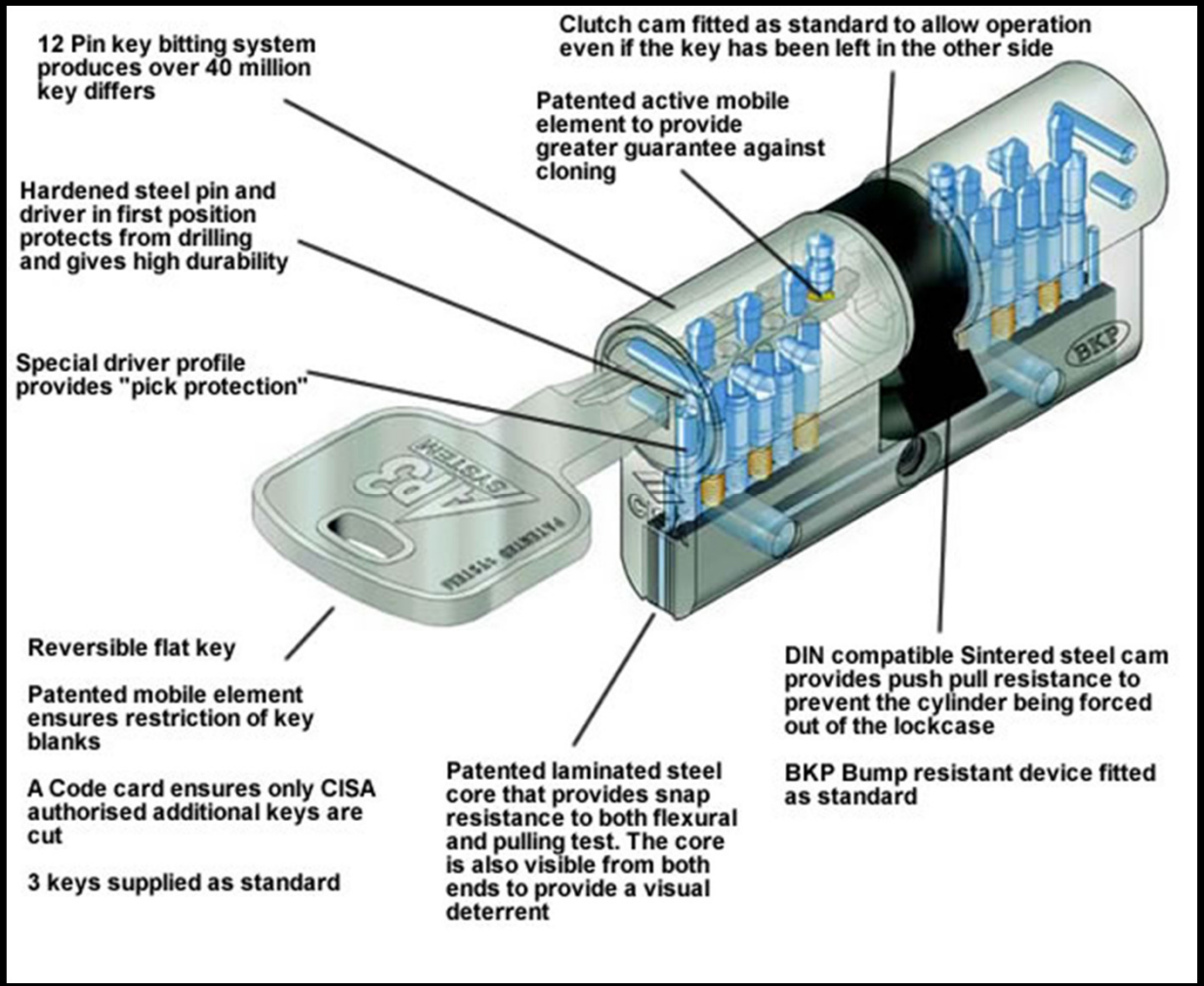
in witness whereof, we have subscribed our signatures to this certificate

GRANTED THIS DAY, 6 October 2004

CERTIFICATE NUMBER 0437233

MARIOS DAMIANIDES
INTERNATIONAL PRESIDENT

RICHARD BRISEBOIS
CHAIR, CERTIFICATION BOARD


12 Pin key bitting system produces over 40 million key differs
Clutch cam fitted as standard to allow operation even if the key has been left in the other side
Patented active mobile element to provide greater guarantee against cloning
Hardened steel pin and driver in first position protects from drilling and gives high durability
Special driver profile provides "pick protection"
Reversible flat key
Patented mobile element ensures restriction of key blanks
A Code card ensures only CISA authorised additional keys are cut
3 keys supplied as standard
Patented laminated steel core that provides snap resistance to both flexural and pulling test. The core is also visible from both ends to provide a visual deterrent
DIN compatible Sintered steel cam provides push pull resistance to prevent the cylinder being forced out of the lockcase
BKP Bump resistant device fitted as standard
BKP

International Information Systems Security Certification Consortium

The (ISC)² Board of Directors hereby awards

William F. Slater, III

the credential of

Certified Information Systems Security Professional

Having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Patricia A. Myers
Chairperson

Recording Secretary

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

CISSP®

ANSI
ISO/IEC 17024

57707
Certificate Number

July 2013
Expiration Date

Certified Since July 2004

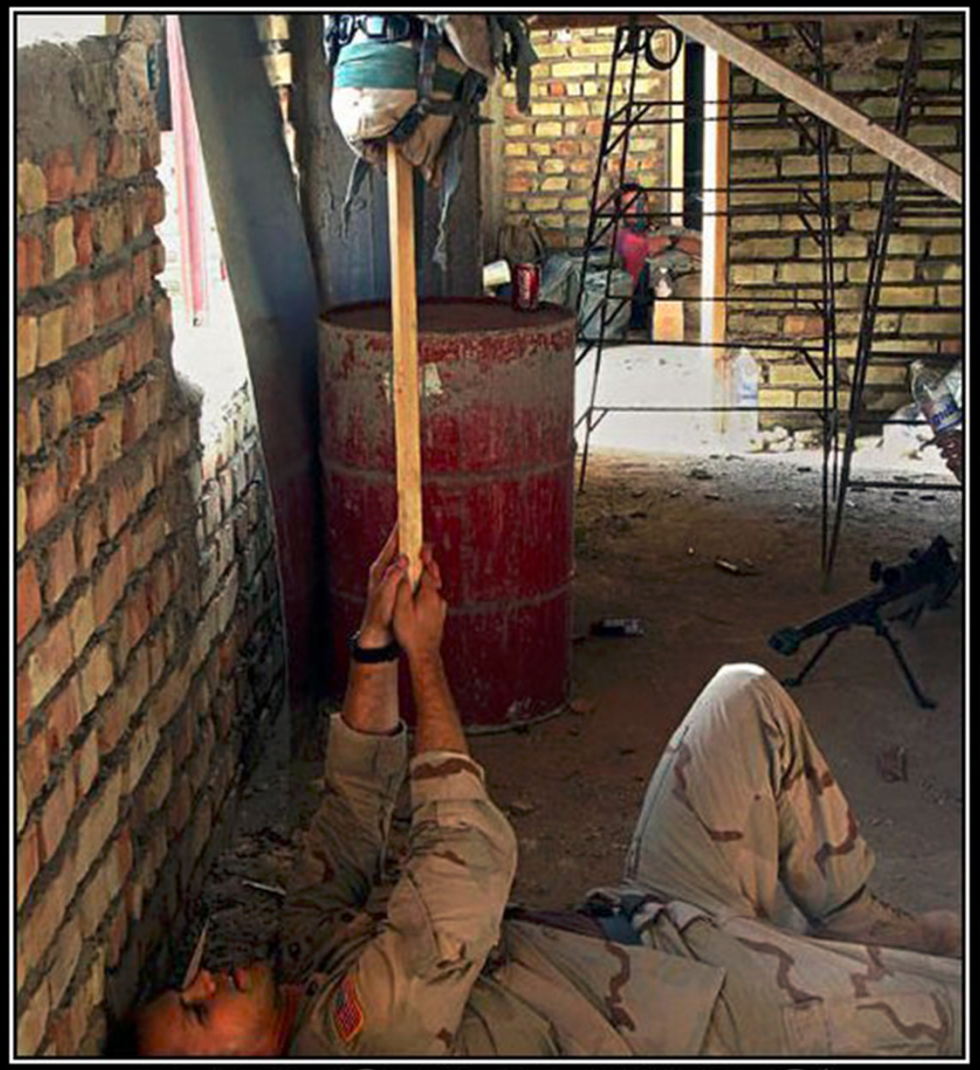
(ISC)²


ISO-27001
Lead Auditor
INFOSEC Assessment Methodology
IAM
INFRAGARD
ASIS
INTERNATIONAL
Advancing Security Worldwide
CELEBRATING 50 YEARS
the CENTER for
INTERNET SECURITY
MEMBER
Information Security Red Team
ISRM
Methodology
BSI
LEAD AUDITORS
PSP®
Physical Security Professional
Board Certified, ASIS International

Does it matter?

Nope.

Don’t like it?



TROLLING

It's kind of like this but on the intarwebs.

Also


HACKING
THE ART OF EXPLOITATION

0day

War Dialing for Dummies

1. Pick up phone

2. Dial phone

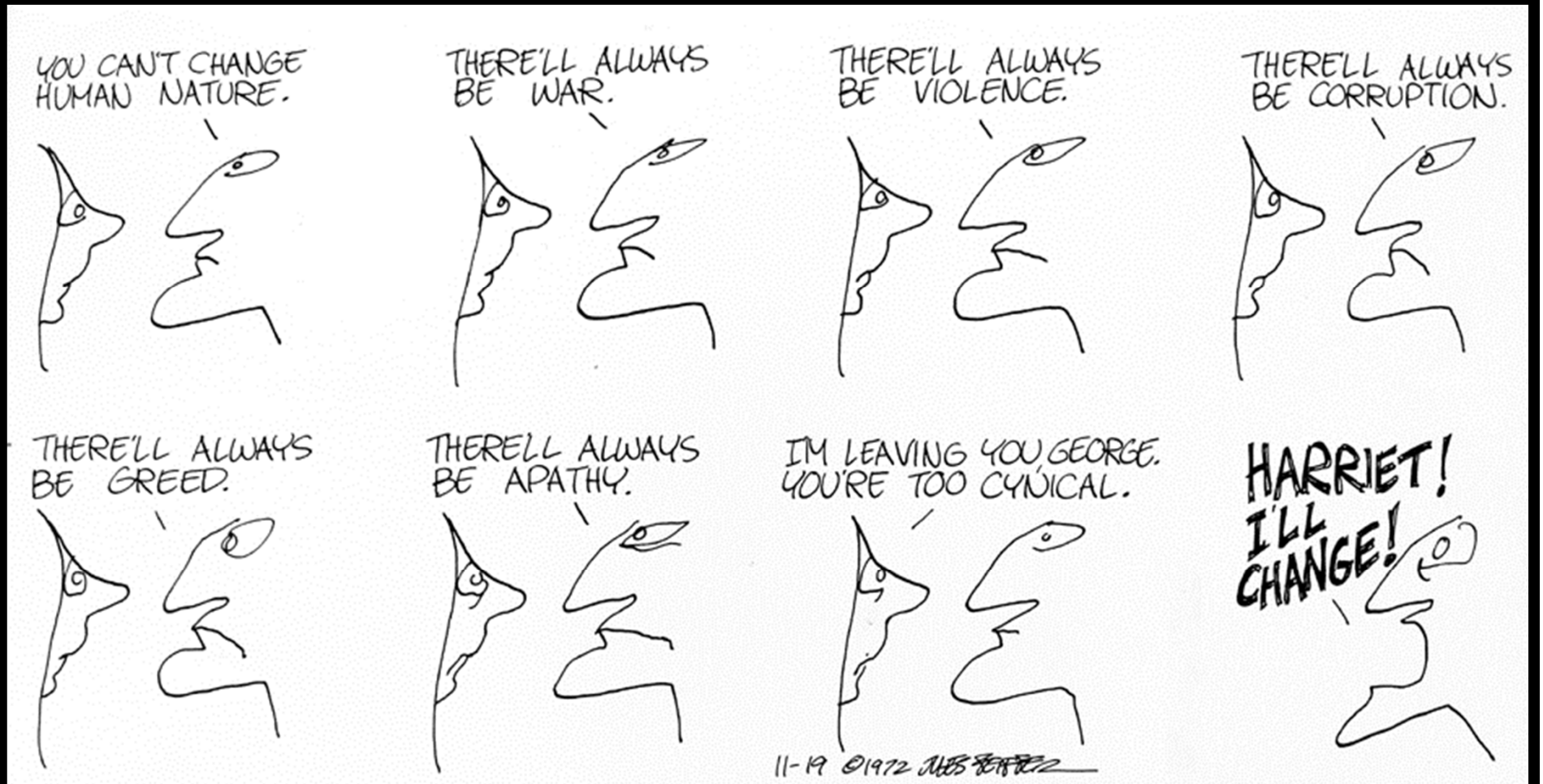
3. Hang up phone

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>


ANDROID
there's a hack for that


Dont wanna do it
Aint gonna do it
U caint make me do it
ICANHASCHEEZBURGER.COM


AUDIT CHECKLIST
Audit Satisfactory
Nonconformances Found
Observations Made


YOU CAN'T CHANGE HUMAN NATURE.
THERE'LL ALWAYS BE WAR.
THERE'LL ALWAYS BE VIOLENCE.
THERE'LL ALWAYS BE CORRUPTION.
THERE'LL ALWAYS BE GREED.
THERE'LL ALWAYS BE APATHY.
I'M LEAVING YOU GEORGE. YOU'RE TOO CYNICAL.
HARRIET! I'LL CHANGE!
11-19 ©1972

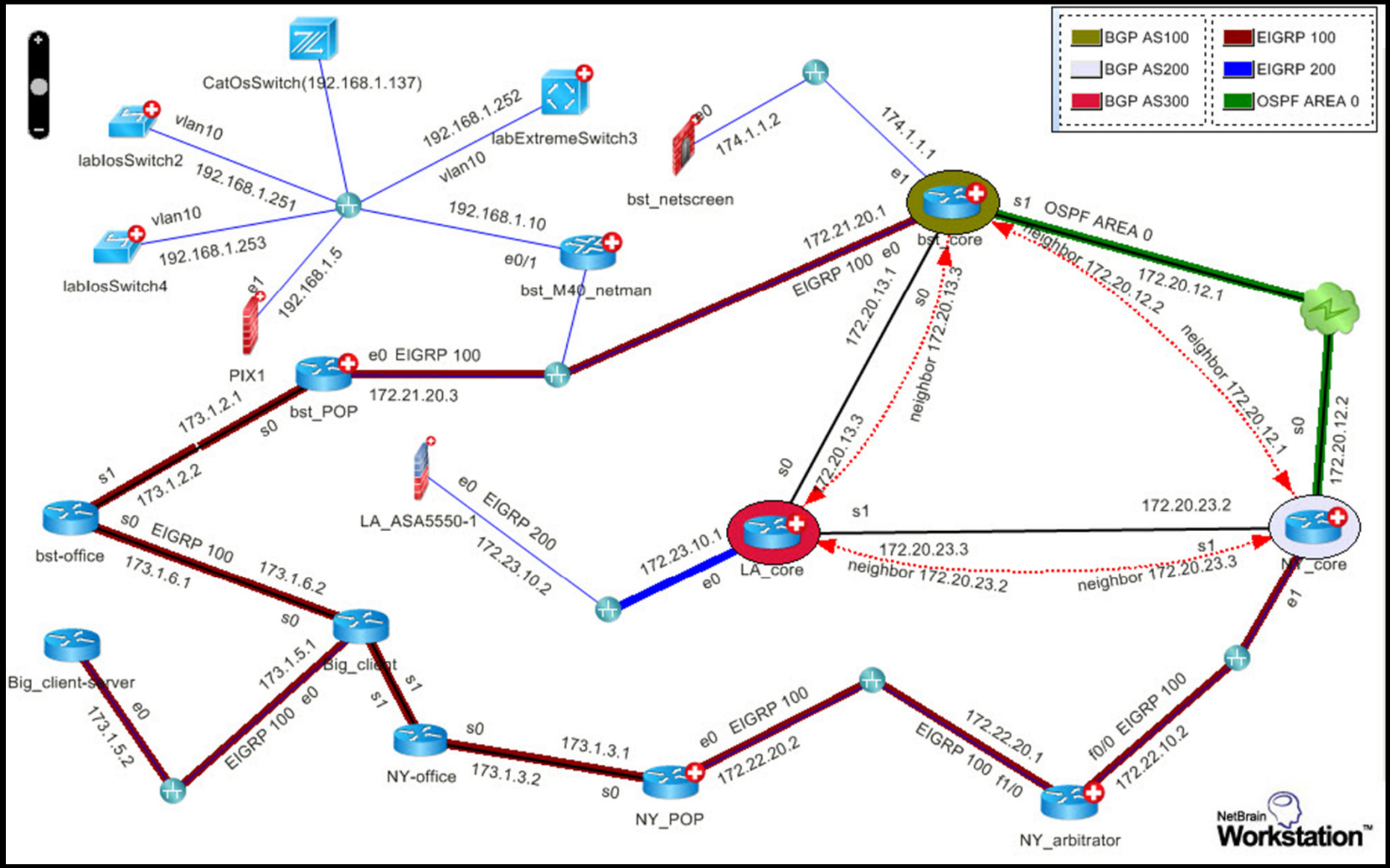
Savage Chickens

by Doug Savage

www.savagechickens.com

CAVEMAN SPEAK

SOME KIDS JUST DON'T GET IT.


BGP AS100
BGP AS200
BGP AS300
EIGRP 100
EIGRP 200
OSPF AREA 0
CatOsSwitch(192.168.1.137)
labIosSwitch2
labExtremeSwitch3
labIosSwitch4
bst_netscreen
bst_M40_netman
PIX1
bst_POP
bst_core
LA_ASA5550-1
LA_core
NY_core
bst-office
Big_client-server
Big_client
NY-office
NY_POP
NY_arbitrator
vlan10
192.168.1.252
192.168.1.251
192.168.1.253
192.168.1.10
192.168.1.5
174.1.1.2
174.1.1.1
172.21.20.1
172.21.20.3
EIGRP 100
OSPF AREA 0
172.20.12.1
172.20.12.2
172.20.13.1
172.20.13.3
neighbor 172.20.13.3
neighbor 172.20.12.1
172.20.23.2
172.20.23.3
neighbor 172.20.23.2
neighbor 172.20.23.3
173.1.2.1
173.1.2.2
173.1.6.1
173.1.6.2
173.1.5.1
173.1.5.2
173.1.3.1
173.1.3.2
172.23.10.1
172.23.10.2
EIGRP 200
172.22.20.1
172.22.20.2
172.22.10.2
NetBrain
Workstation™

Like any new thing

Its Scary

We need to feel SAFE!

So


RULES
1. YOU CAN....
2. YOU CAN'T...
3. YOU CAN....
4. YOU CAN'T


©Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
EDGAR-ARGO
"YOU'RE WRONG!... RULES ARE NOT JUST ROUGH GUIDELINES."


STANDARDS


Best Practices

COMPLIANCE

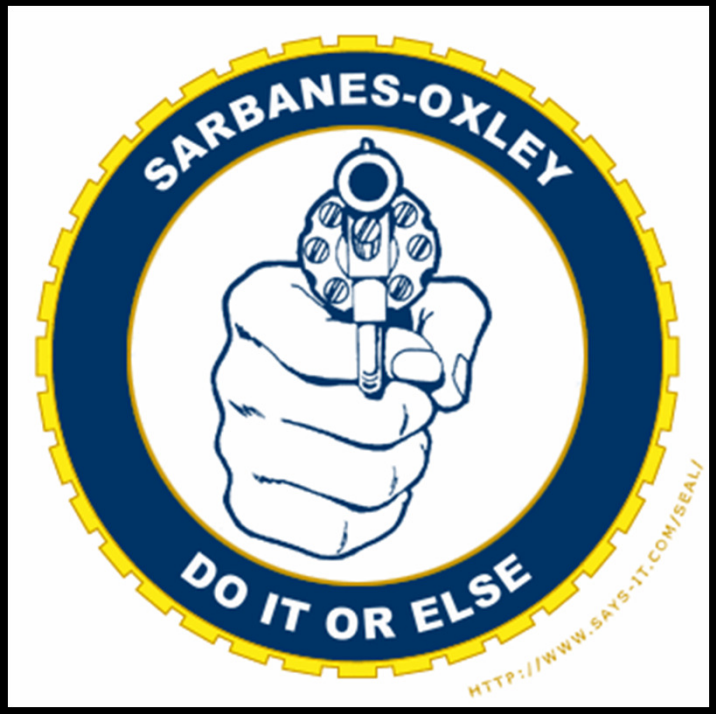
We will NOT...
Oh wait, maybe we will.

Trivia?

From that moment on..


A.KURTZ
HOMELAND SECURITY BLANKET

So they created some new standards for us to live by

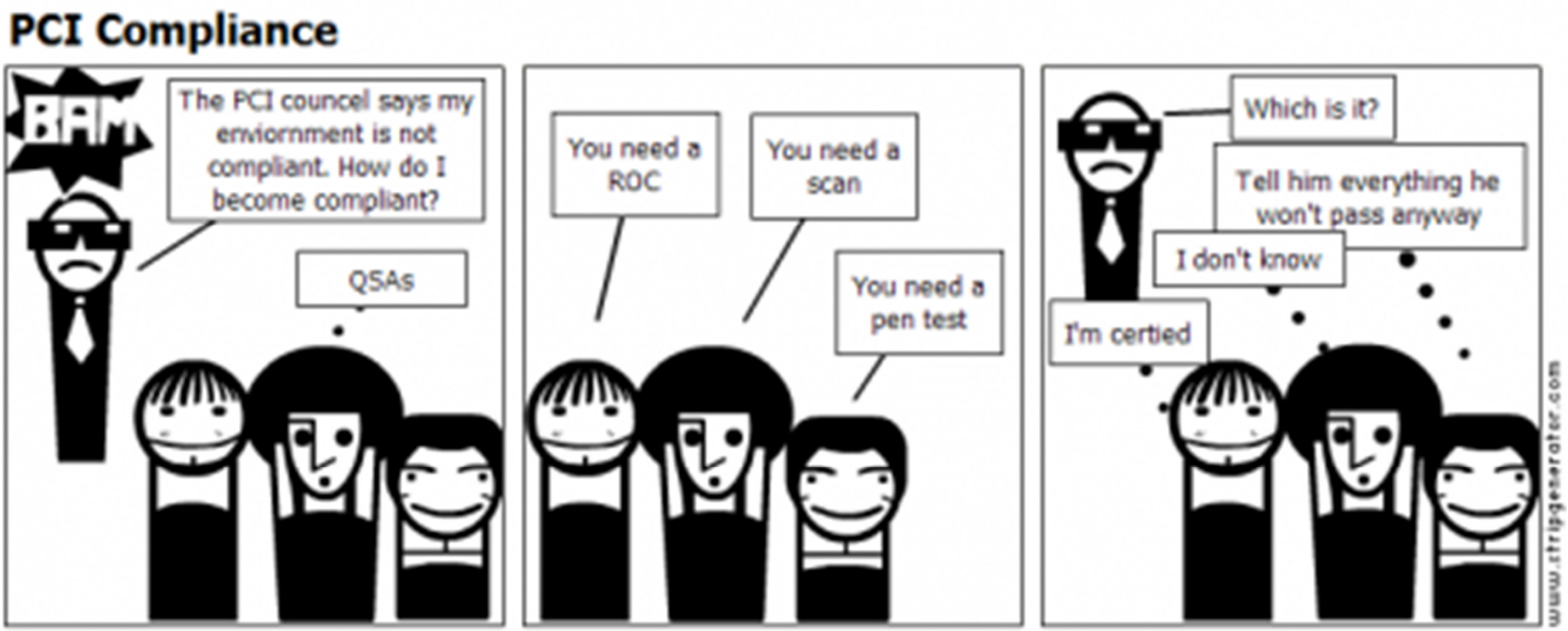


SARBANES-OXLEY

Implement controls to Protect the validity of Financial reporting

HIPAA

Implement controls to Protect PHI



PCI

Implement controls to Protect Credit Card Data

HITECH

Implement controls OR You will have to disclose that PHI was compromised

NIST

PRESIDENT'S COMMISSION *on* CRITICAL INFRASTRUCTURE PROTECTION

FIPS 140-2 LEVEL 3 VALIDATED

FDIC

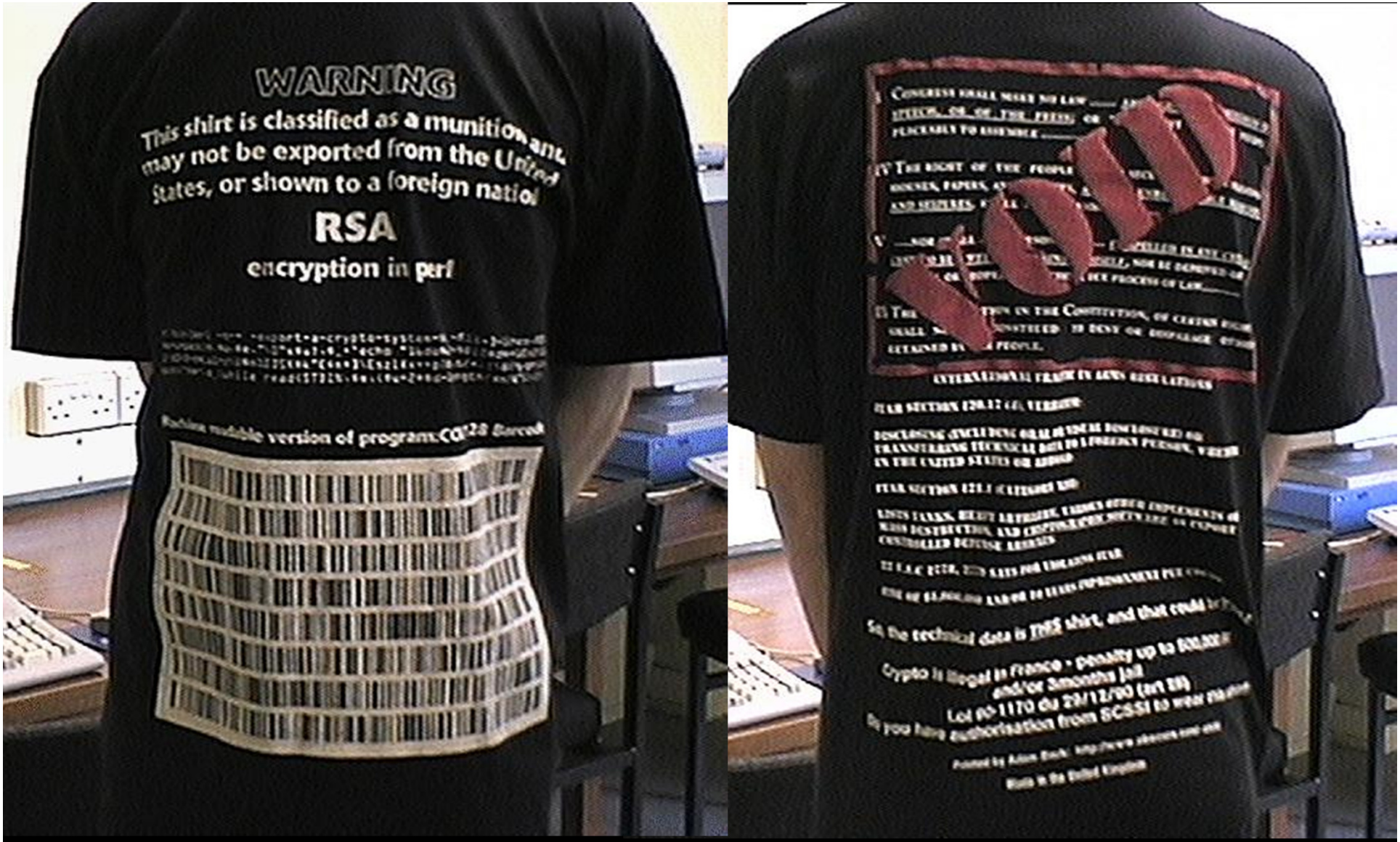
RAL DEPOSIT INSURANCE CORPORATION

COBIT®
GOVERNANCE, CONTROL *and* AUDIT *for* INFORMATION *and* RELATED TECHNOLOGY


ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES


MEANWHILE
BACK AT THE RANCH

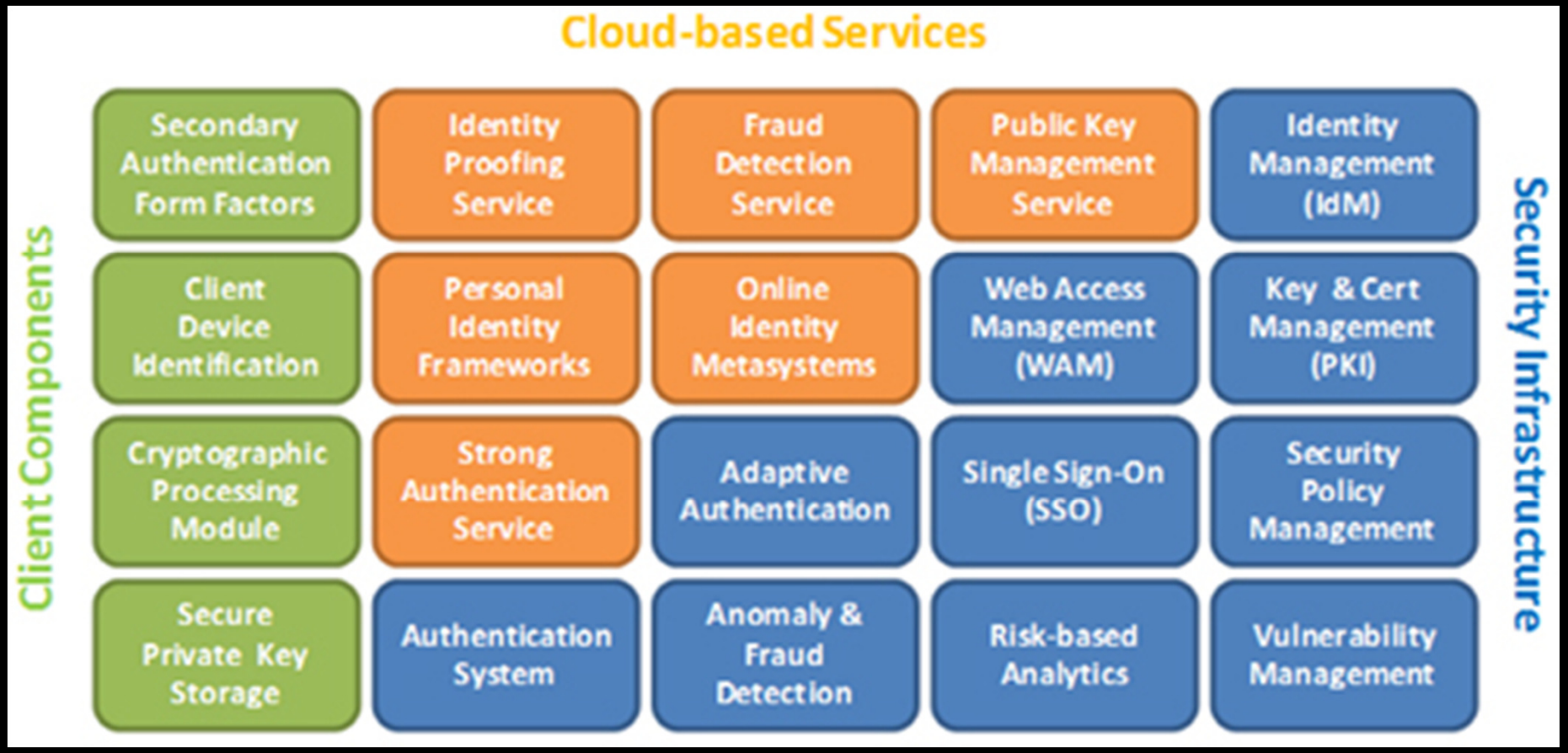

NAYER
THE UNITED STATES OF AMERICA
ONE DOLLAR


WARNING
This shirt is classified as a munitions and
may not be exported from the United
States, or shown to a foreign nation
RSA
encryption in perl
Machine readable version of program:
So the technical data is THIS shirt, and that could
Crypto is illegal in France - penalty up to
and/or 3months jail
Loi 90-1170 du 29/12/90 (art 28)
Do you have authorisation from SCSSI to wear
Printed in the United Kingdom

ENCRYPTION


Intrusion Detection & Prevention Systems

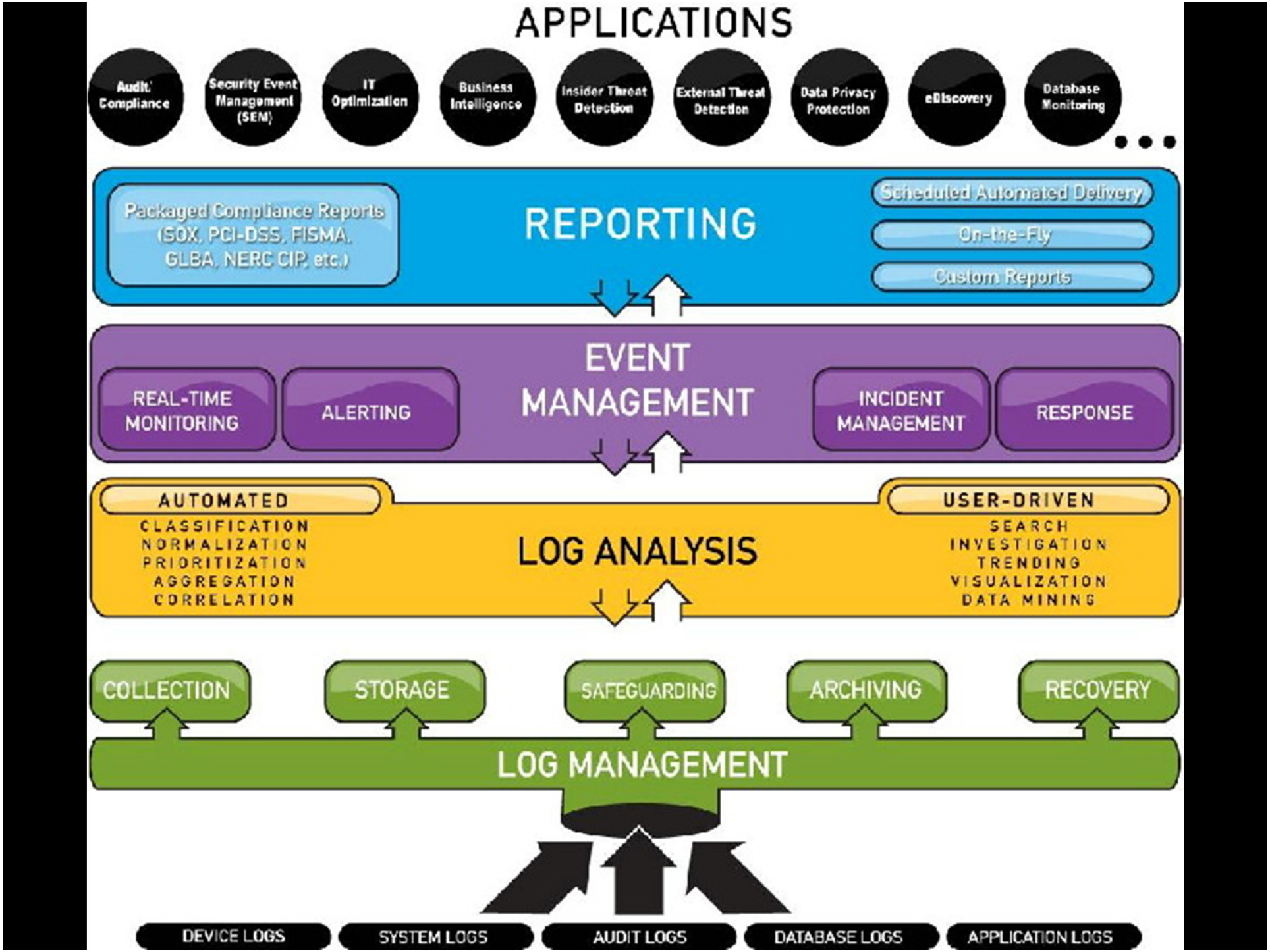
AV/Anti-Badware


Cloud-based Services
Client Components
Security Infrastructure
Secondary Authentication Form Factors
Identity Proofing Service
Fraud Detection Service
Public Key Management Service
Identity Management (IdM)
Client Device Identification
Personal Identity Frameworks
Online Identity Metasystems
Web Access Management (WAM)
Key & Cert Management (PKI)
Cryptographic Processing Module
Strong Authentication Service
Adaptive Authentication
Single Sign-On (SSO)
Security Policy Management
Secure Private Key Storage
Authentication System
Anomaly & Fraud Detection
Risk-based Analytics
Vulnerability Management

Strong Auth

INTEGRITY

The guy with the pet crow looks after all their money.


APPLICATIONS
Audit/ Compliance
Security Event Management (SEM)
IT Optimization
Business Intelligence
Insider Threat Detection
External Threat Detection
Data Privacy Protection
eDiscovery
Database Monitoring
Packaged Compliance Reports (SOX, PCI-DSS, FISMA, GLBA, NERC CIP, etc.)
REPORTING
Scheduled Automated Delivery
On-the-Fly
Custom Reports
REAL-TIME MONITORING
ALERTING
EVENT MANAGEMENT
INCIDENT MANAGEMENT
RESPONSE
AUTOMATED
CLASSIFICATION
NORMALIZATION
PRIORITIZATION
AGGREGATION
CORRELATION
LOG ANALYSIS
USER-DRIVEN
SEARCH
INVESTIGATION
TRENDING
VISUALIZATION
DATA MINING
COLLECTION
STORAGE
SAFEGUARDING
ARCHIVING
RECOVERY
LOG MANAGEMENT
DEVICE LOGS
SYSTEM LOGS
AUDIT LOGS
DATABASE LOGS
APPLICATION LOGS


EVERYTHING HE LOVES IS
ABOUT TO BE USED AGAINST HIM.
FIREWALL
© 2006 WARNER BROS. ENTERTAINMENT

Trivia Round 2

Of the
6
Top Firewalls
How many can
effectively
block TCP ports?

1

As proven by NSS labs testing in April 2011. Web briefing today Thursday, April 21, 10am-11am PDT

NSS Labs
Security. Certified.


No one likes Sad Panda.

Other than make us sad…

What has all this done for us?

Made corporations aware of the risk

THANK YOU!!!!

Misdirected security funding and goals

(80% of the budget for security is spent on 5% of the assets for compliance)

tp://iang.org/papers/market_for_silver

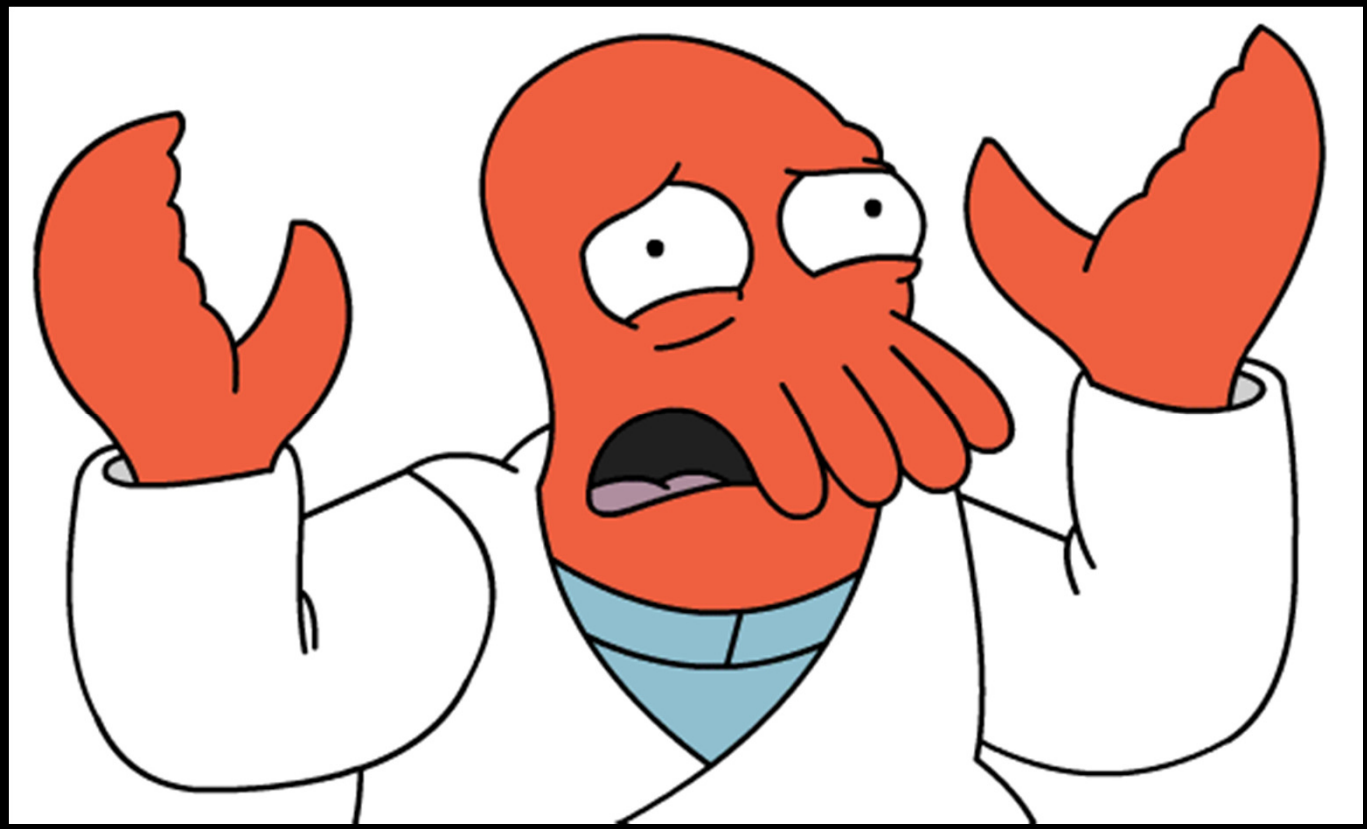
http://www.schneier.com/blog/archives/2

BLAME

THE SECRET TO SUCCESS IS KNOWING WHO TO BLAME FOR YOUR FAILURES.

Urgent

Unimportant



_____ YOU!!!!

Why doesn't it work?

Inefficient

We have our sights set on compliance NOT SECURITY

Criminals want us to suck at security

Illegal drug market: est. $400 billion

Cybercrime market: est. $600+ billion


Bad Guys
Compliance


LOST
CONFUSED
UNSURE
UNCLEAR
PERPLEXED
DISORIENTED
BEWILDERED

Focus on, protecting what matters **MOST** to the company

What **DO** they care about?

You don't always know…
Admit it!

THE PRODUCT LINE

THE BRAND

THE EMPLOYEES

THE BOTTOM LINE

HOW To identify what to protect and test

STEP #1 YOUR OPINION DOESN'T MATTER

ASSIMILATION

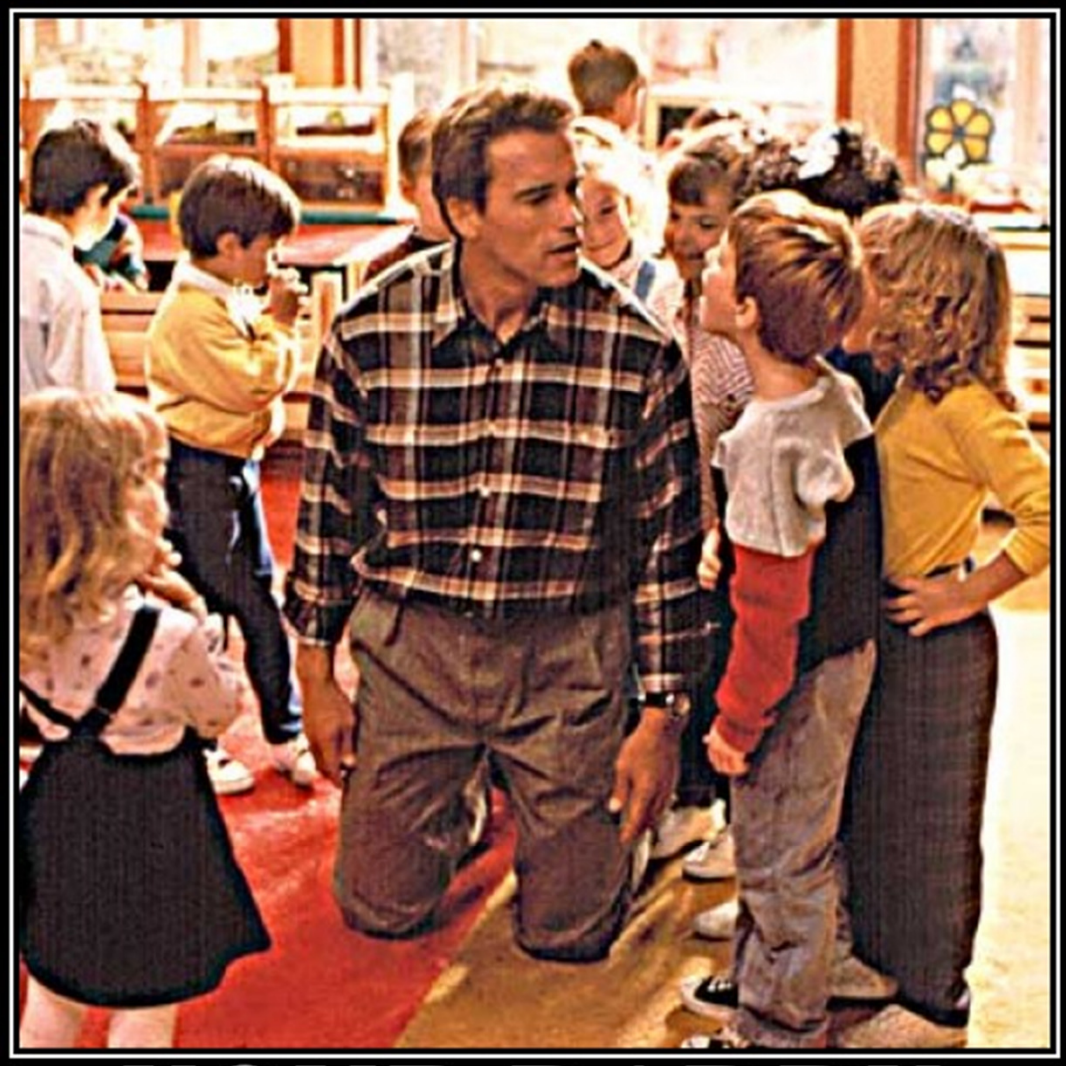
All your ship are belong to us.

STEP #2 THINK LIKE “THEM”

STEP #3: DO WORK

Yea... this is the boring stuff...but u gotta do it....

FOCUS ON THE BUSINESS



YOUR DADDY

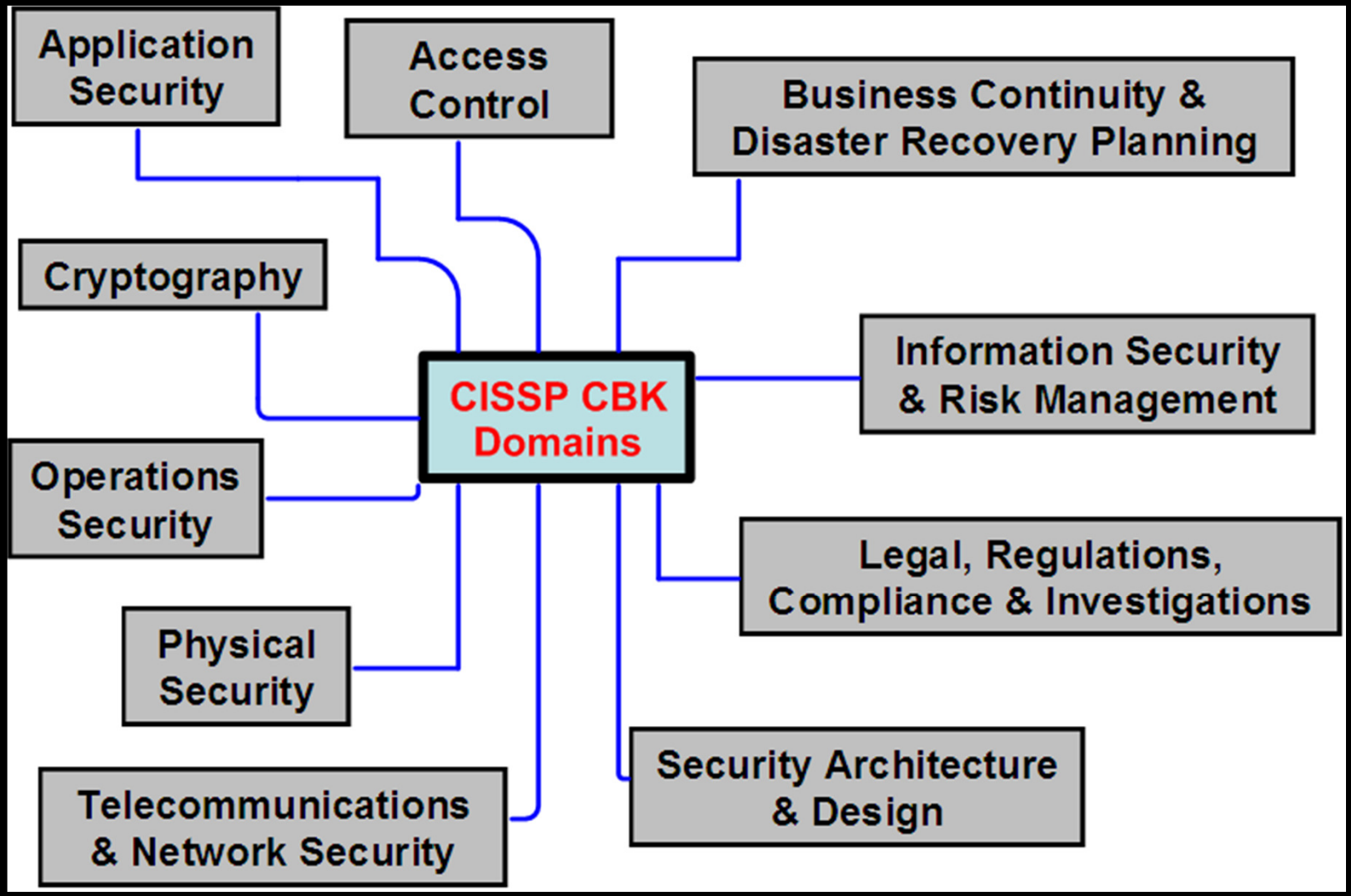
who is he and what does he do?

WHAT ARE YOUR PRODUCTS? HOW DOES YOUR TESTING AND/OR SECURITY STRATEGY INCREASE THEIR PROTECTION

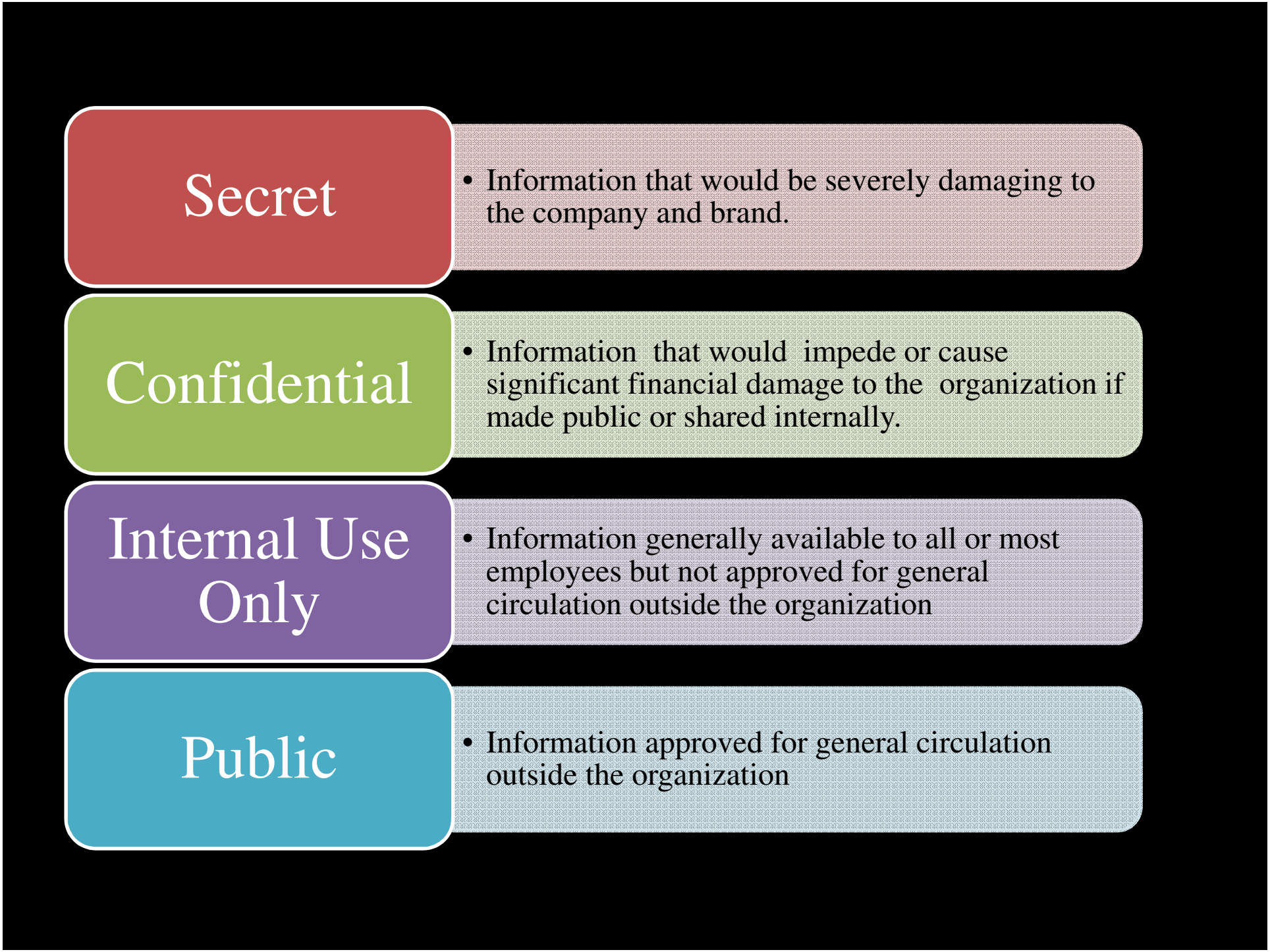
IDENTIFY WHERE
YOUR $ COMES FROM
AND WHERE IT GOES

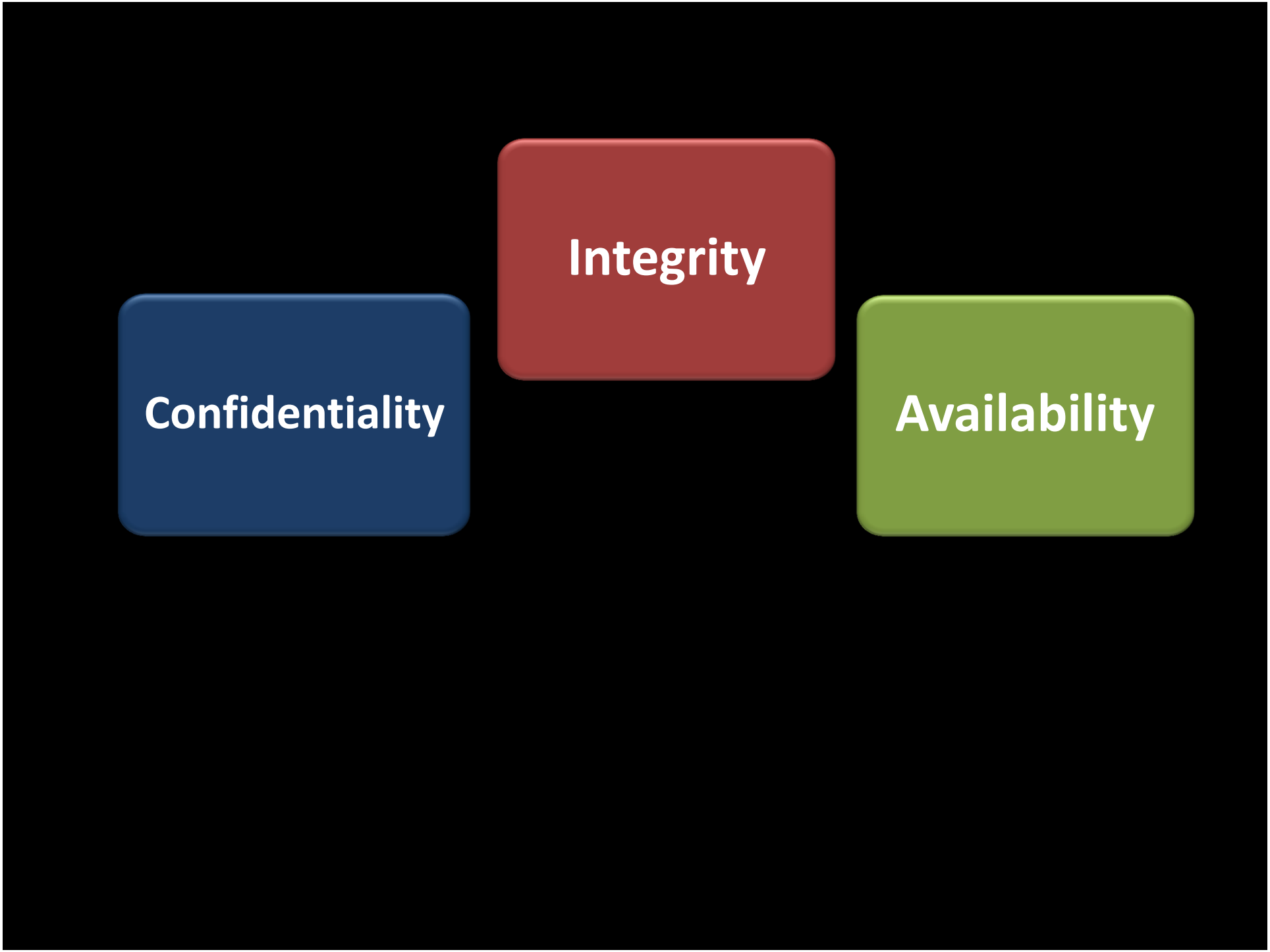

Last login: Mar 12 07:03:29 on console
Welcome to os4!
> telnet -a -b ABSOLUT 192.168.100.1:8080
> enter login: #####
> enter passw: #####
> invalid passw ERROR (retype)
> retype passw #######
> OK you are SUCCESFULLY logged in
> cd /usr/.ABSOLUT/SECRETS
> ls -l -a BACKDOORVIRUSES
-rwxr-xr-- TROJANHORSE#BF1 - 306 Mar 7 20:55
-r-xr-xr-- TROJANHORSE#CA0 - 1026 Mar 11 00:13
-r-xr-xr-- TROJANHORSE#CB9 - 716 Mar 5 14:15
-rwxrw-r-- TROJANHORSE#CFF - 4865 Feb 9 22:06
-r-xr--r-- TROJANHORSE#D2C - 48 Jan 28 17:24
-r-xr--r-- TROJANHORSE#D8A - 512 Mar 2 02:22
-r-xr-xr-x TROJANHORSE#DA6 - 512 Mar 7 04:46
-r-xr--r-- TROJANHORSE#DD7 - 642 Feb 13 01:58
-r-xr--r-- TROJANHORSE#DF2 - 1784 Dec 31 11:33
-rwxr--r-- TROJANHORSE#EA3 - 1256 Mar 4 14:56
-rwxrw-r-- TROJANHORSE#EB4 - 2873 Mar 5 08:17
-r-xr--r-- TROJANHORSE#ED8 - 255 Feb 17 10:45
-r-xr--r-- TROJANHORSE#FA3 - 207 Feb 17 10:57
> sudo -sP TROJANHORSE#D2C
System is about to reboot
Killing all processes .....
ABSOLUT HACKER.
ABSOLUT COUNTRY OF SWEDEN VODKA & LOGO, ABSOLUT, ABSOLUT BOTTLE DESIGN AND ABSOLUT CALLIGRAPHY ARE TRADEMARKS OWNED BY VIN & SPRIT AB. THOSE WHO APPRECIATE QUALITY ENJOY IT RESPONSIBLY. THIS AD WAS MADE BY PIXY 2003.

DO YOU HAVE A COMPETITOR? WHAT WOULD THEY WANT TO HAVE ACCESS TO?



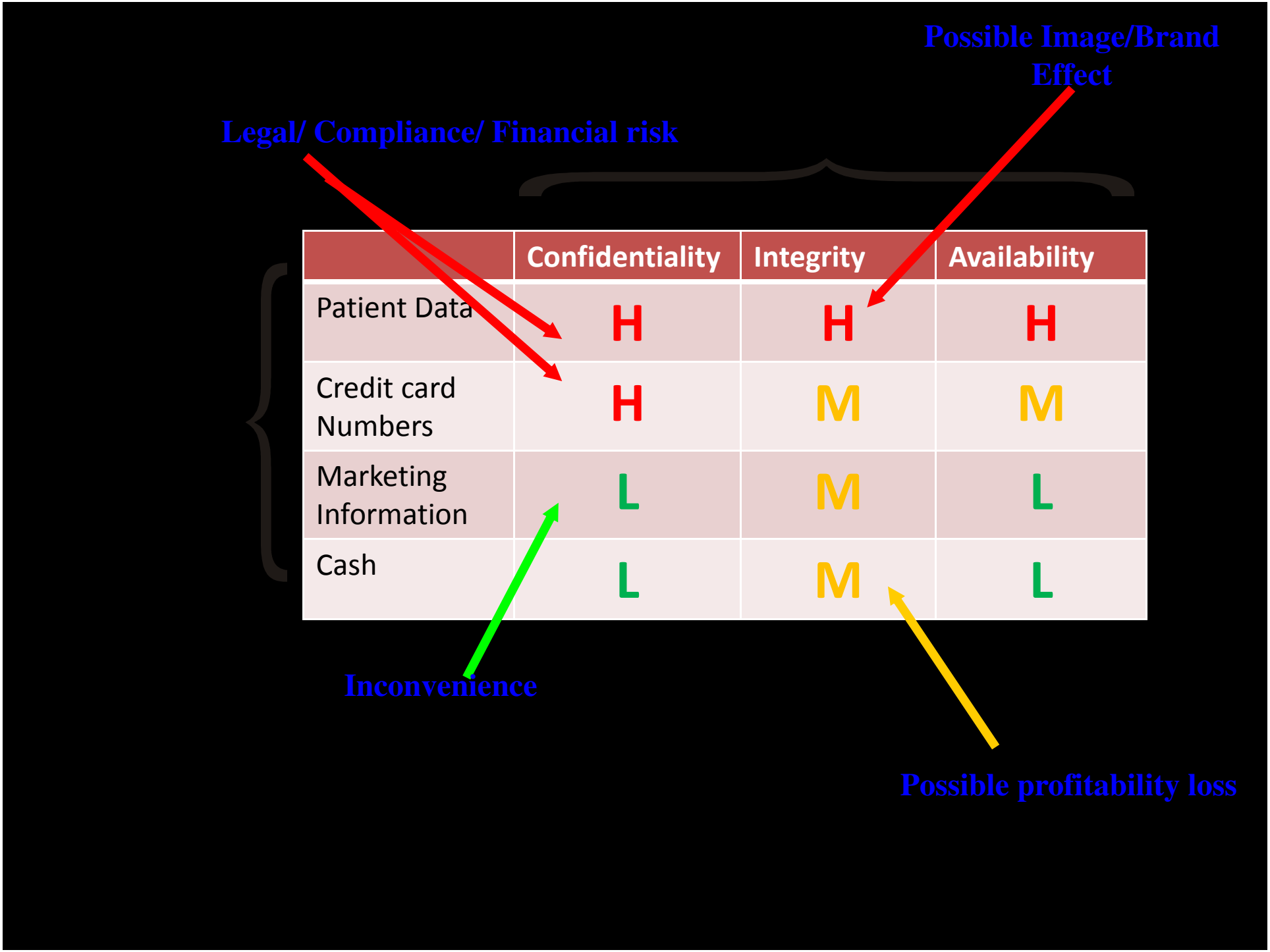
Ok… Too simple? How bout we go all formal then?


Secret
• Information that would be severely damaging to the company and brand.
Confidential
• Information that would impede or cause significant financial damage to the organization if made public or shared internally.
Internal Use Only
• Information generally available to all or most employees but not approved for general circulation outside the organization
Public
• Information approved for general circulation outside the organization


Integrity
Confidentiality
Availability


Integrity
Confidentiality
Availability
Criticality

	Confidentiality	Integrity	Availability
Patient Data			
Credit card Numbers			
Marketing Information			
Cash			



	Confidentiality	Integrity	Availability
Patient Data	H	H	H
Credit card Numbers	H	M	M
Marketing Information	L	M	L
Cash	L	M	L

Changed to H after conversation of how it impacts profitability

	Confidentiality	Integrity	Availability	SCORE
Patient Data	H	H	H	5
Credit card Numbers	H	M	M	4.3
Marketing Information	M	M	L	1.6
Cash	L	M	L	1.6

Changed to L after conversation of how it was already public information

HIGH	**5**
MEDIUM	3
LOW	1

HOLY S#*t!!!
THAT PART WAS BORING

But we had to do it to make sure we have a PROCESS to let them tell us what they care about……. Even when **they** don't know what it is…

Let’s get real*


LOST
abc


F0J3052605
TEN · DOLLARS · DIX
TWENTY

TOTALLY UNFAIR

Never let a Jedi in the Olympics

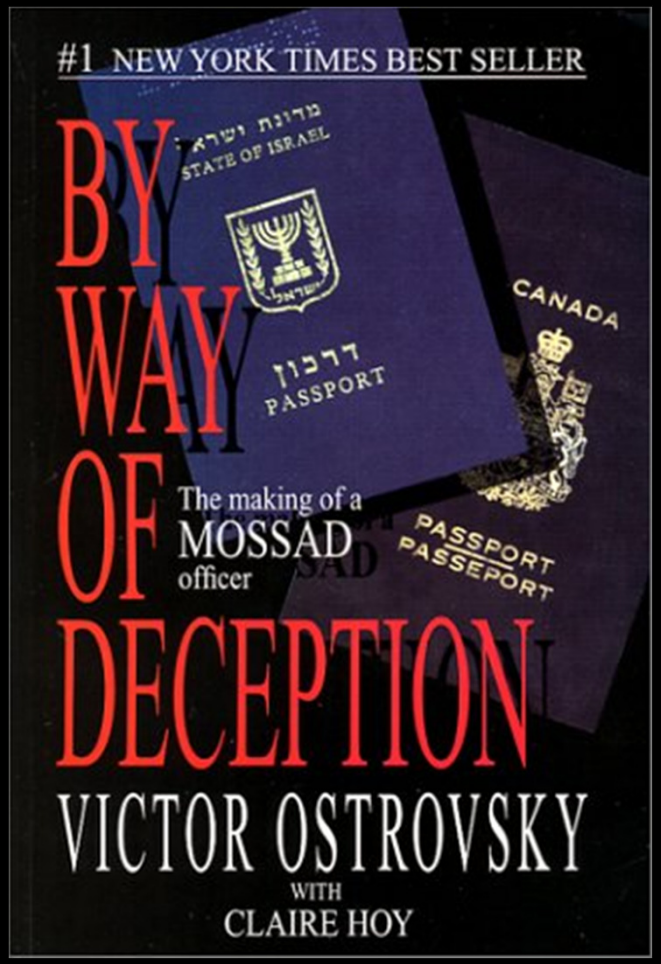
INFORMATION SECURITY PROGRAMS ARE A PHYSICAL MANIFESTATION OF OUR OWN VANITY

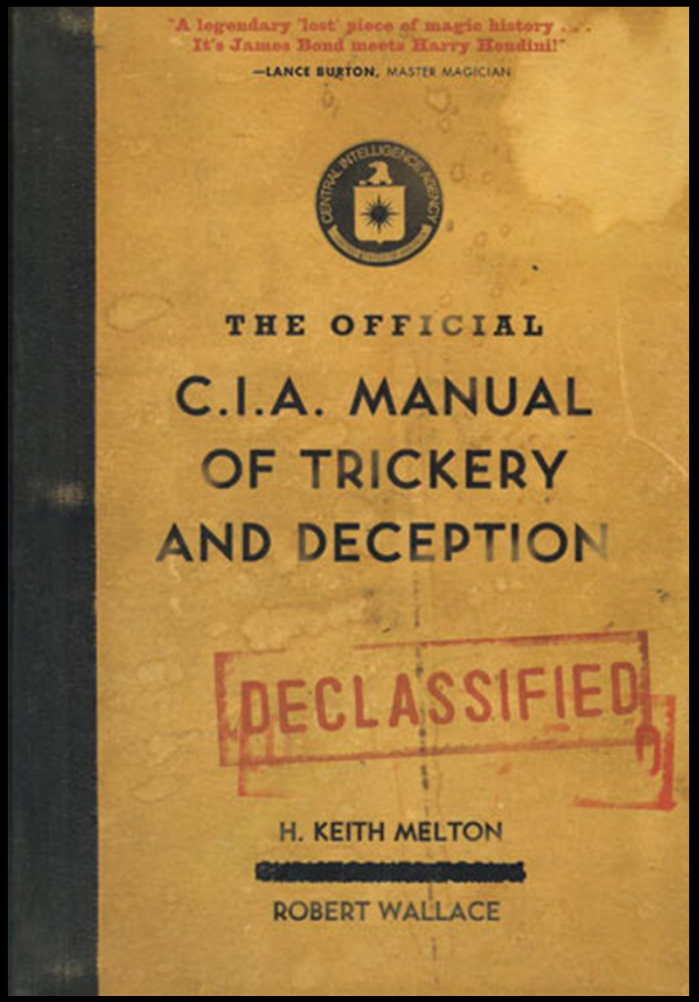
Thanks tim


UFC
UFC
HCK

STEP 0

EDUCATION

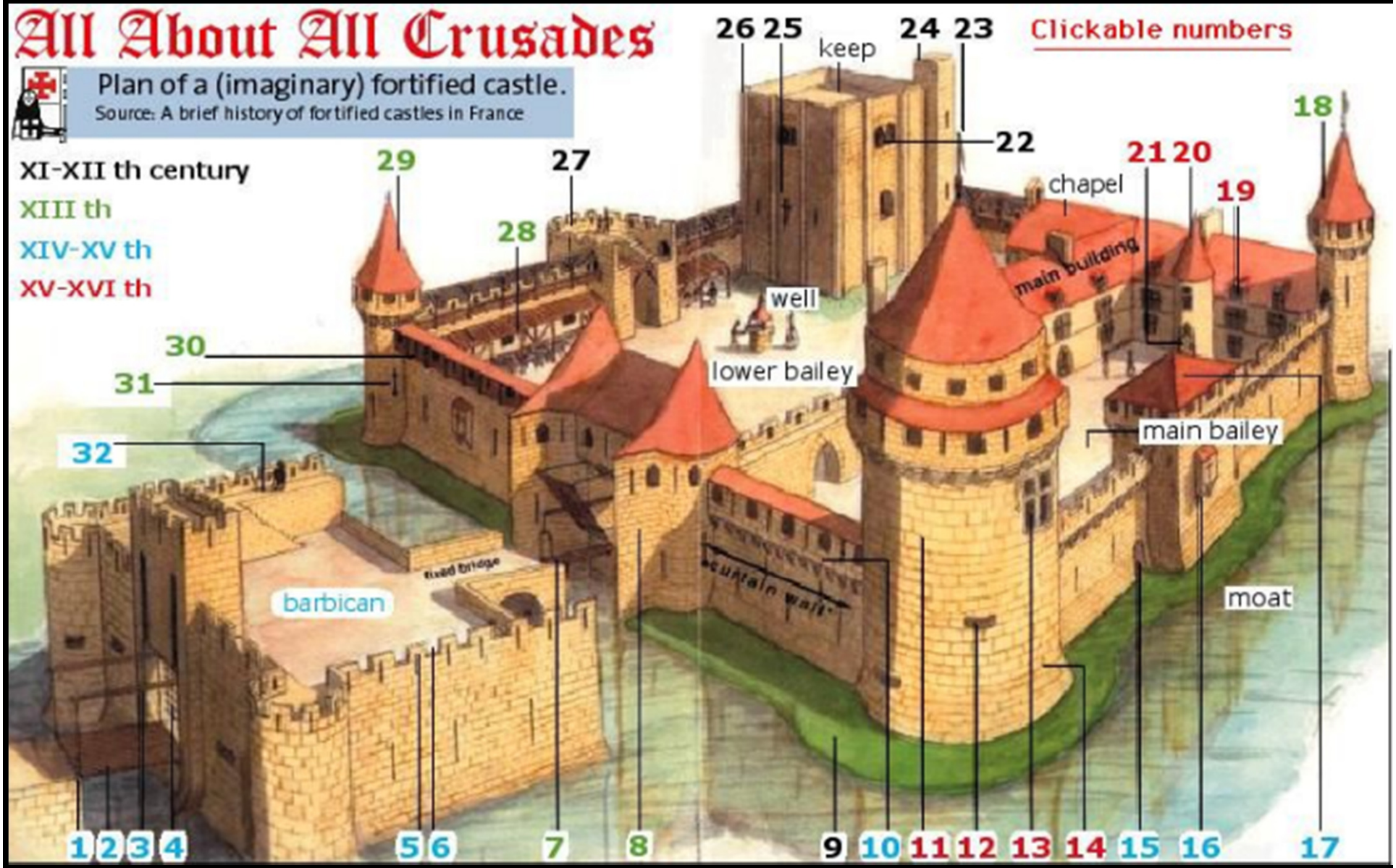

#1 NEW YORK TIMES BEST SELLER
BY WAY OF DECEPTION
The making of a MOSSAD officer
STATE OF ISRAEL
PASSPORT
CANADA
PASSPORT
PASSEPORT
VICTOR OSTROVSKY
WITH
CLAIRE HOY


"A legendary 'lost' piece of magic history . . .
It's James Bond meets Harry Houdini!"
—LANCE BURTON, MASTER MAGICIAN
THE OFFICIAL
C.I.A. MANUAL OF TRICKERY AND DECEPTION
DECLASSIFIED
H. KEITH MELTON
ROBERT WALLACE

DECEPTION

Hide where you're least likely to be found

All About All Crusades



What do you have to lose?

YOU HAVE
ALREADY BEEN
HACKED

D95-21(MOD)

“GOD,
grant me the serenity to
accept people that will
not secure their
networks, the courage to
face them when they
blame me for their
problems, and the wisdom
go out partyin’
afterwards!”

1. We admitted we were powerless over security - that our environments had become unmanageable.

2. Came to believe that a power greater than ourselves could restore us to being secure

3. Made a decision to turn our will and our lives over to the care of best practice as we understand them.

4. Made a searching and fearless inventory of our environments and its assets, both information and physical.

5. Admitted to ourselves and those assisting us in our recovery the exact natures of our wrongs

6. Were entirely ready to have an independent assessment of our environment and accept the recommendations suggested to remove the flaws identified.

7. Humbly ask for help remediating our flaws.

8. Made a list of all the persons we ignored and became willing to make amends to them all

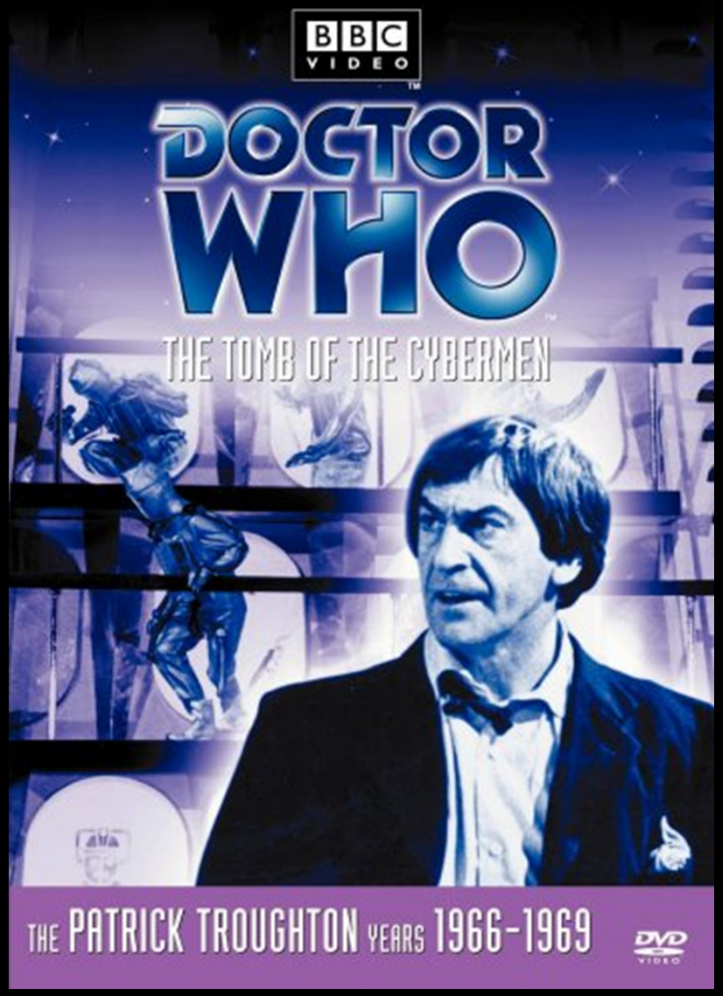
9. Made direct amends to such people wherever possible, except when to do so would injure the brand or the company.

10. Continue to take corporate inventory and when we were find flaws promptly admitted it

11. Sought through policy, process and procedure to improve our conscious understanding of best practices as we understand them and only for knowledge of its will for us and the power to carry that out

12. Having had a corporate awakening as the result of these steps, we tried to carry this message to other organizations and to practice these principles in all our affairs

Time to move on to something new and get over the past we fear is our future.



"The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious" - Dr. WHO