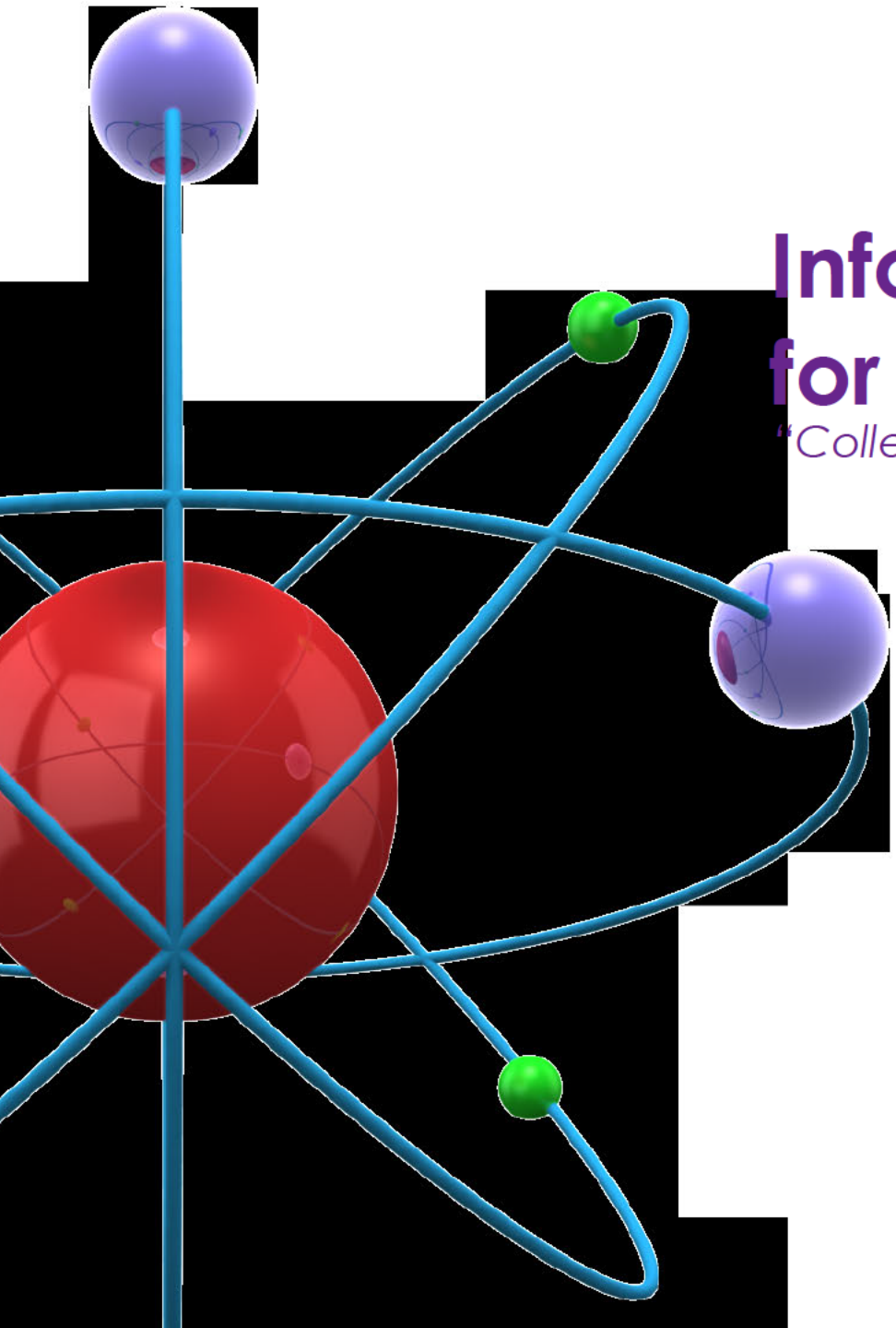


Information Warfare for the Corporation

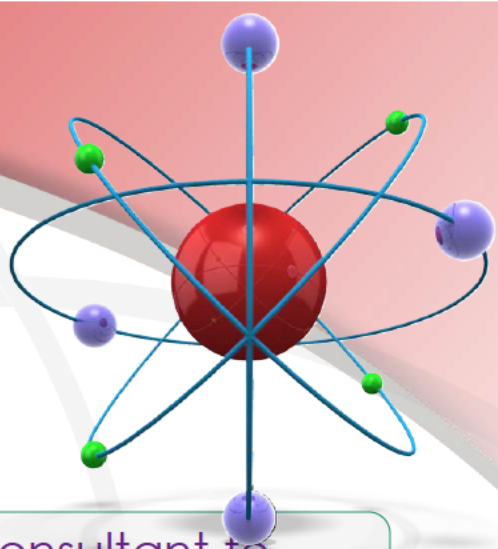
"Collection" as a corporate option

NEbraskaCERT May 2013

By KC Fredman

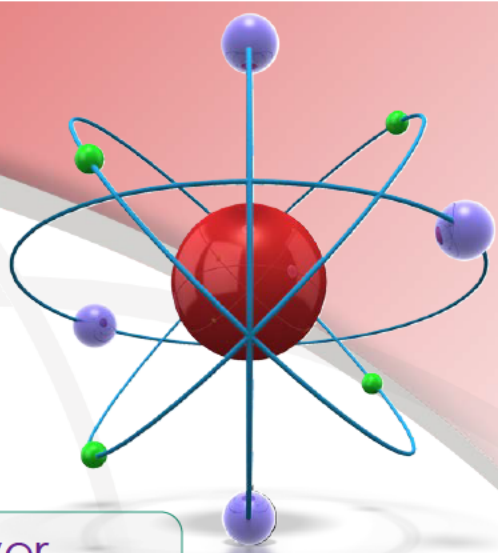
About me

Will hack 4 food



- Professional InfoSec researcher and consultant to public and private organizations
- Professor of Cyber Security Studies
- Avid Listener
- Lifelong Learner

•Caveat



These are my thoughts only; not of any employer former or present

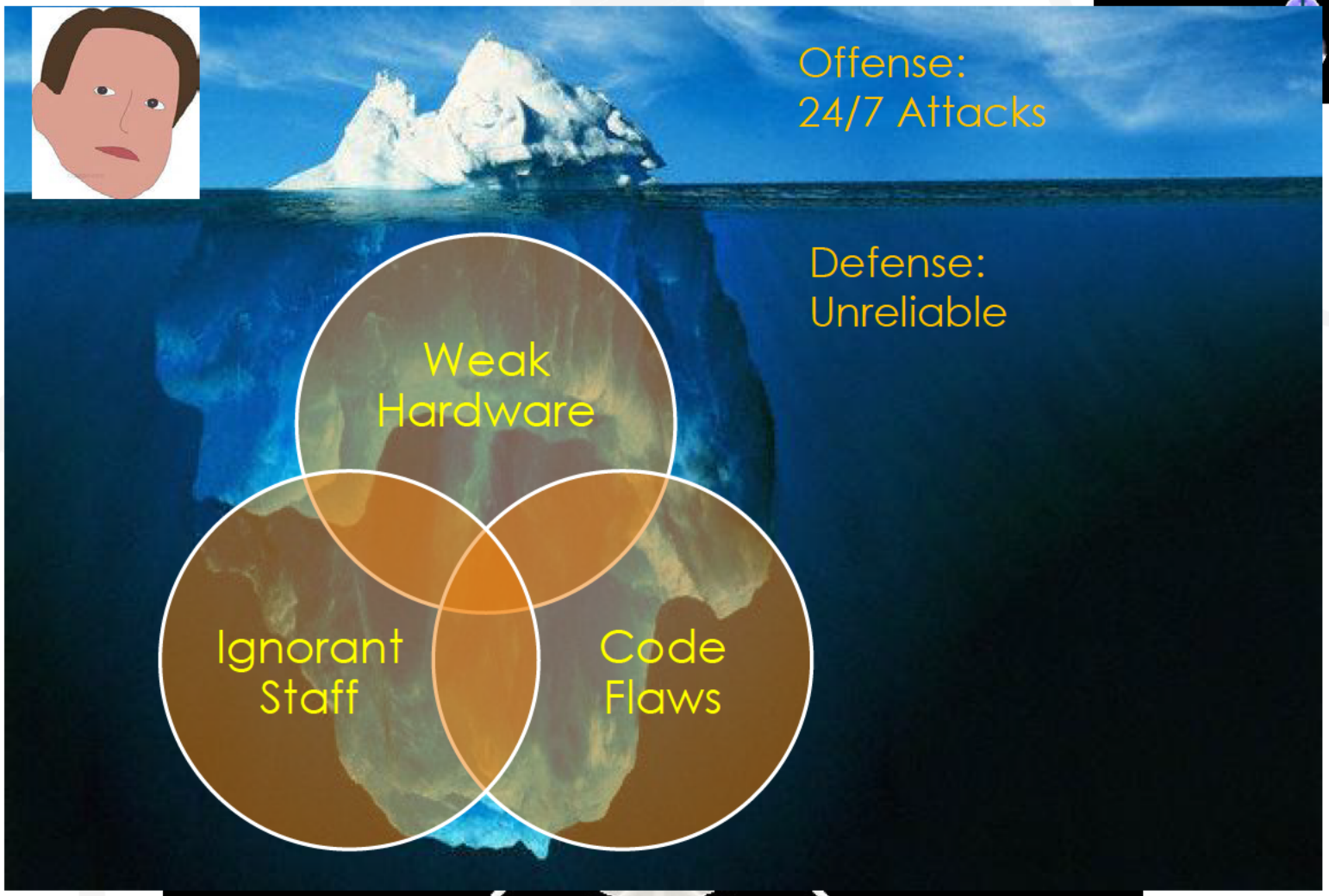
Every Corporation has lawful duties and must maintain those at every endeavor

Always consult with legal experts and include them as team members

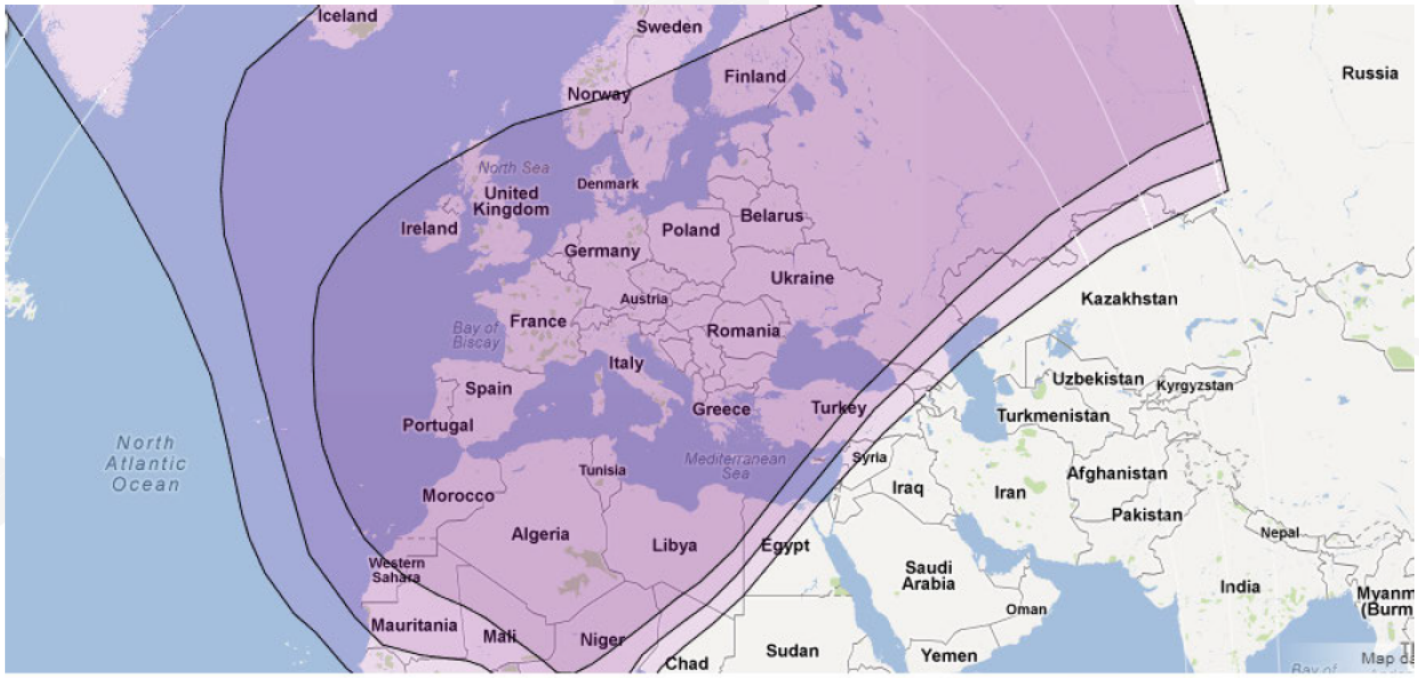
- **The basic rule of strategic conflict**

The offense always wins.

•The inconvenient Truth



•Sidebar..Internet Research



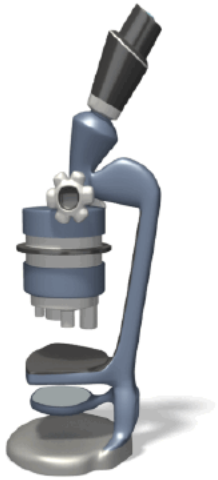
According to a website listing Satellites, this is one that was launched to provide TV services to Eastern Asia.

•Missing in the corporation???

- Intelligence Gathering
  - The first step in intelligence chain effectiveness
  - You're not just being breached. Someone is breaching you – who is it?
- Intelligence Reach
  - Not a mere dissemination to a manager

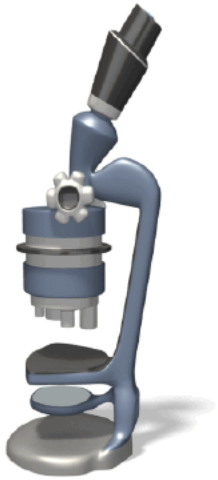
Wisdom begins with the definition of terms – Socrates

(Un)Familiar Terms in the Context of InfoSec



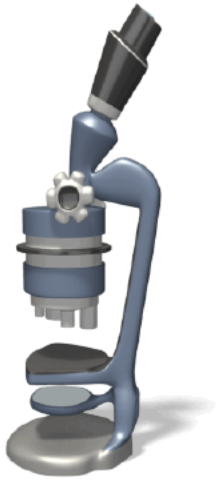
- Access Agent – Algorithm used to acquire target information
- Access – The approach of the operational asset performing CI within the limits of acceptable risk
- Special Access Program (SAP) – The "backdoor"
- Advisory Tasking – Collection notices gathered by internal/external partners

(Un)Familiar Terms in the Context of InfoSec



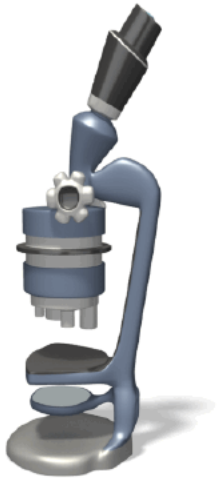
- All-Source – The combined product of Intelligence Gathering
- Anomalous Activity – IT "Stuff" outside of the expected norms
- Assessment Product – In depth cyber analysis with qualified judgments
- Assumption – The traditional pentest report

(Un)Familiar Terms in the Context of InfoSec



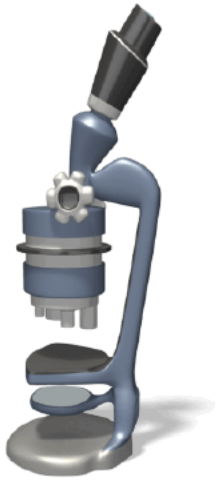
- Basic Intelligence – Log Aggregation Information; past reports; attack reference material
- Black List – Identities of IP's determined to be loose ends.
- Control – Offensive measure to modify unintended algorithms without deletion
- Counterintelligence – Activities conducted to identify rogue attackers, and the information gathered from those activities

(Un)Familiar Terms in the Context of InfoSec



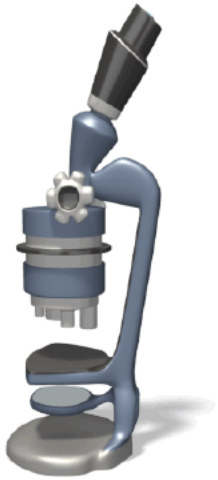
- Countermeasure – negating the ability to exploit the architecture
- Cyber incident – an undesired security incident (effective or otherwise)
- Damage Assessment – The written analysis on the effects of a compromise
- Handler – the corporate analyst responsible for cyber information gathering

(Un)Familiar Terms in the Context of InfoSec



- Intelligence Cycle – The process of acquiring information and converting it to intelligence for decision makers
- Judgment – Information that fills that gaps to cope with uncertainty
- Rabbit – The target on the other end
- Red Team – Corporate element of educated and trained individuals working as a collective to gather intelligence

(Un)Familiar Terms in the Context of InfoSec



- Multi-person Integrity – Prohibiting the ability of information gathering to one individual
- Open Source – Publically available information that anyone can lawfully obtain
- Tag – Something attached to a backdoor that is phoning home
- Validation – Confirming that defensive efforts are not being duplicated

•Sidebar…Essential Hacking tools

- Alias(es)
- Linux
- Scripting languages
- Local Proxy
- Universal Proxy – proxy chaining

Intelligence is about Conflict

- It's not about being right or wrong

Conflict has three areas of capacity

1. Prevention
   - Making an existing situation more advantageous
2. Deterrence
   - When preventative measure fail
3. Defeat
   - Resolving an intrusion in a custom way

•Today's corporate process issues

1. Information is outdated before it gets to the lower level managers
2. Information gets passed through bulky processes like 6sigma and SDLC's
3. A breach seems irrelevant unless is affects PCI/DSS
4. Appropriate positions or resources are not used to establish intelligence (attack intel not business intel)
5. Ignorance is a common feature in management

Defense in Depth????

It's concentration is merely a diversion

1. Defend the Networks
   - Confidentiality and Integrity
2. Defend the Enclave Boundaries
   - Firewalls, WAF's, IDS, IPS, …
3. Defend the Computing Environment
   - Access Controls…

Defense in Depth????

Ignores offensive controls

Defend the Computing Environment

- Access Control – (Note: See the OWASP cheatsheet)
- Deploy WAF's – (We can't patch, let's do it virtual)
- Deploy IDS/IPS (There's never an anomaly)
- Other semi-useful hardware made for salespeople

Defense in Depth

It is based on apparent and known threats

What it gets right is the basic premise of 3 "pillars"

- People
- Technology
- Operations

Defense in Depth

What is missing?

It sets up the wrong train of thought

That is, Attackers are reliable, Defenders are NOT

Defense inherently disregards Offense; Offense heeds Defense

Point 1

We need to put the reliability into Offensive Capabilities and subsequently back into the hands of the corporation or business

Deception for Intelligence Gathering

Could be useful

What if we owned XYZ corporation and hopped on an IRC channel, with known criminals, submitting the following message:

"www.xyzcorporation.com/users.php has a really cool SQL injection"

Deception for Intelligence Gathering

XYZ's blog post is meant for two outcomes:

1. Gathering Information
2. Hacking the hacker

Who is watching you?

Organizations should expect that "someone" is always studying them for weaknesses

1. Everything you say is/can be recorded
2. Loose lips sink ships

•Four True Sources of Intelligence

- Open Source
  - What is said is not as important as who said
- HUMINT
  - Dealing with illicit networks (commercial espionage)
- COMINT
  - Generally illegal for private entities
- Cyber Collections
  - The vast amount of information from logs as well as hacking ones own systems

•Important to know

- Data
  - Unprocessed fact or fiction
- Information
  - "Validated" Data
- Knowledge
  - Information "once analyzed and understood" that alllows comprehension to take place (Referred to as Intelligence in the DoD)

•Unique Exploits are not being addressed

- Example
  - Multi-varient virus – this is how it's accomplished

- Capture a common virus
- Take it apart into 100-500 *.exes
- Locate the signatures
- Replace the signatures with XOR or 00
- Recompile – and send it on its way

- You have a new virus that the AV vendors don't have

•Why do we fail at Defense in Depth?

- Attack information is from secondary sources
- Too much subjectivity in collections
- Infrastructures are too big and diverse
- Applications for defense aren't truly vetted

Point 2

Reliance and Subjectivity are the factors of failure

•Corporate Intelligence Reach

First, it allows analysts to easily retrieve essential pieces of security data

Next, the data is evaluated against other data (e.g. PCI Reports, pentests)

Next, it is dissemenated to relevant team members for report construction

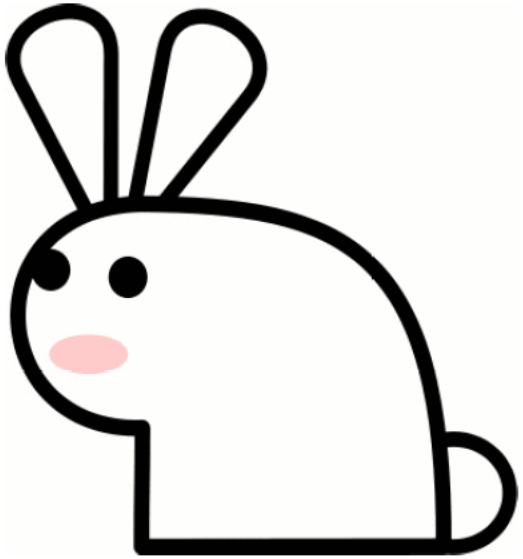
Finally, it is provided to appropriate executives

•Intelligence Gathering for the Corporation

- Is not defensive but rather proactive
- Can eliminate threats rather than defend against them
- Can be done without affecting the opposition

An example – the backdoor

- Countermeasure
  - Common option – shut down and replace server
  - Uncommon option – Tag and Control the Rabbit



•Could be based on defensive rather than offensive

If the goal is gathering intelligence, then you are not "taking them down"

It cannot be deterrence based

It could be deception based

- US based companies cannot do it

•The next security paradigm

Detecting the Undetectable

Walking with the intruder

Following the intruder home

The wrong(illegal) model in the corporate world is infiltrating another's system to cause harm

- "The ultimate goal of Stratagem is to make the enemy quite certain, very decisive and wrong," Barton Whaley

•Suggested Readings

- *How to Break a Terrorist* - Mathew Alexander
- *Images and Intervention* – Martha Cottam
- *The Masks of War* – Carl H. Builder
- *Why Intelligence Fails* – Robert Jervis
- *Influence – Science and Practice* – Allyn & Bacon

Questions?