Everything I know about Information Security, I learned from my Sentry Dog

Ed Crowley, Sentry Dog Handler

US Army ‘69-’71

http://www.youtube.com/watch?v=u_23RoeJfI0

https://www.youtube.com/watch?v=ZqD4Fx5P86w

Today's Topics

- Sentry Dog Security
- A Simple Risk Model
  - Risk and Risk Primitives
- NIST Cybersecurity Perspective
- Current Context
  - Feeling Secure vs Being Secure
- Security and Deterrence
- Accountability on the Internet
- Selected Threats
- Selected Vulnerabilities
- Summary
  - For Further Study

Selected Qualifications

- Certified Ethical Hacker – EcCouncil
- AccessData Certified Examiner – AccessData Forensic Tool Kit (FTK)
- Certified Information Systems Security Professional (CISSP) – ISC^2
  - Usual Cisco, CompTIA, and Microsoft Certifications
  - CCNA, Security +, Internet +, Network +, MCSE
- Graduate:
  - USARPAC Basic Sentry Dog School
  - US Army Military Police Academy
- Wrote first UH Info Security Curriculum.
  - First UH Curriculum certified by the NSA and the Committee on National Security Systems (CNSS).

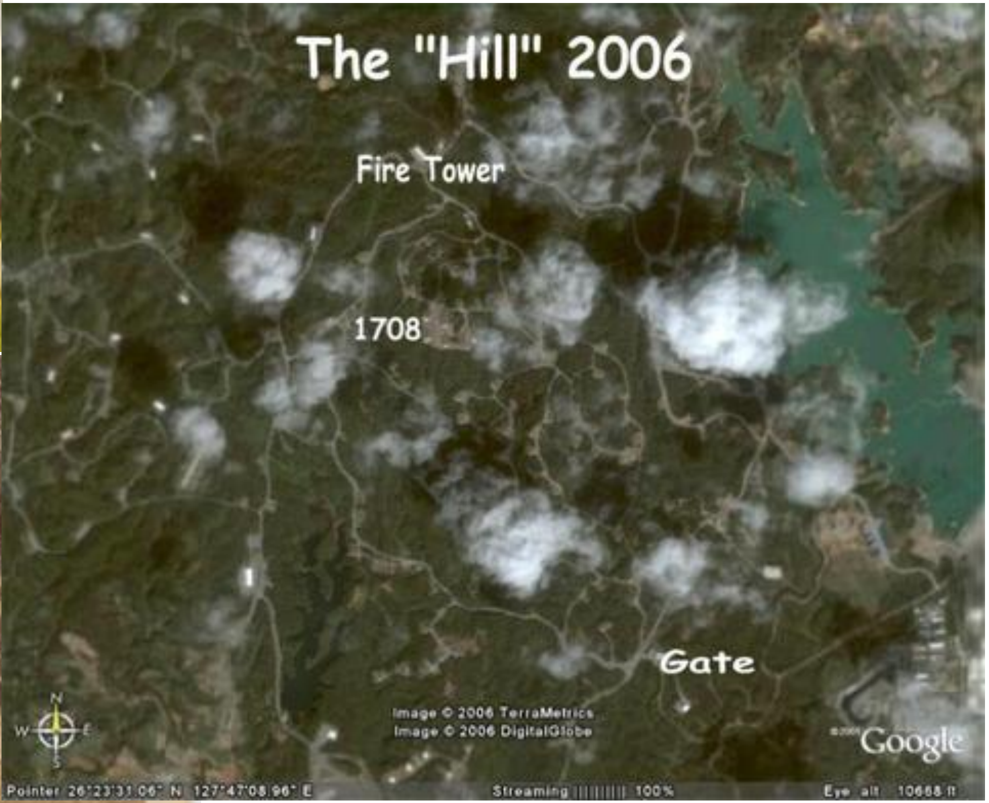
War Dogs ‘69

- Training intense
- Working conditions deplorable
- Lives always on the line
- … Rewards non-existent [1.]

1. http://www.uswardogs.org/war-dog-history/vietnam/

US Army, '69-'71

Sentry Dog Platoon, 267th Chemical Co.


The "Hill" 2006
Fire Tower
1708
Gate
Image © 2006 TerraMetrics
Image © 2006 DigitalGlobe
Google
Pointer 26°23'31.06" N 127°47'08.96" E
Streaming 100%
Eye alt 10668 ft

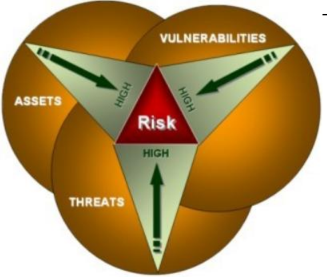
3.2 mile perimeter. 10 meter dead area. One gate, locked and manned 24/7 . Southern Okinawa highest hill. Overlooked Kadena Air Base. Enough Nerve Gas to kill everyone in the world, three times.

Ref: 267th Chemical Company or Operation Red Hat

Nemo
A534

Risk Models

- German Shepherds are born with an effective Risk Model. You're not.
- Models provide means to move feeling and reality closer together. But first:
  - What is risk?
  - What is security?
  - Let's define our terms…



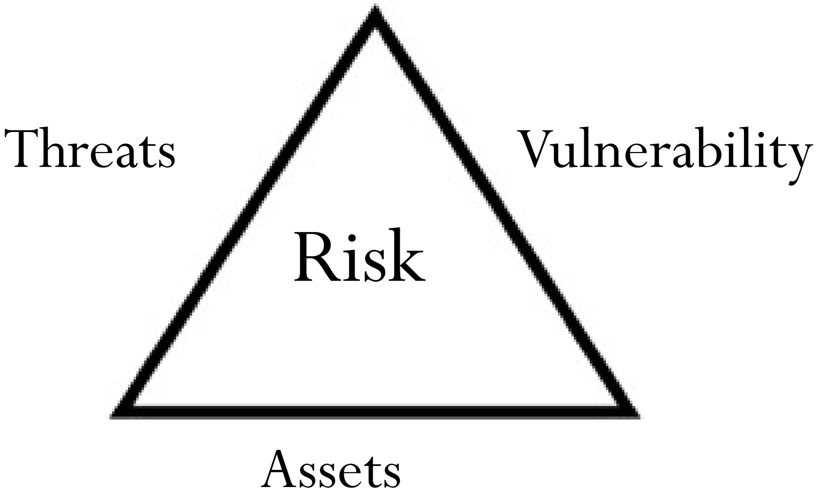
Risk & Risk Primitives

- Vulnerability
  - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security …
- Threat
  - Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.
- Asset
  - A definable piece of information, stored in any manner which is recognized as 'valuable' to the organization.
- Risk
  - The probability that a particular threat will exploit a particular vulnerability …

- *NCSC-TG-004 Aqua Book*
  - *See also RFC 2828*

If you know your assets, threats, and vulnerabilities, you can calculate your risk.
NIST SP 800-30 Guide for Conducting Risk Assessment.

A Simple Risk Model



For any given situation, the risk is proportional to the area of a triangle formed by the assets to be protected, the threats to the assets, and the current vulnerabilities.

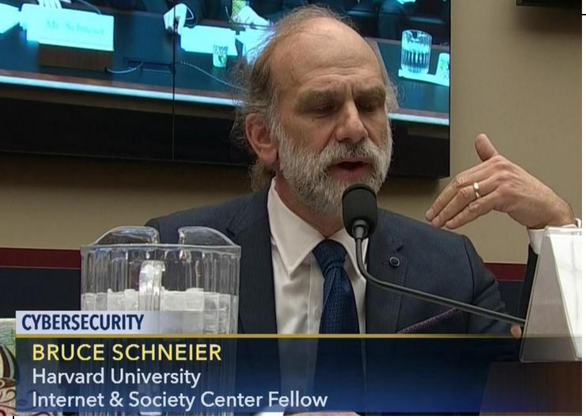
- A metric consisting of your enterprise's threats, vulnerabilities, and assets at a particular time would be called your security posture.
- Normally security posture determined through a Risk Assessment.

Computer Security Golden Rules

Three golden rules to ensure computer security

1. Do not own a computer.
2. Do not power it on.
3. Do not use it.

–Robert H. Morris, *who in the early 80's, served as Chief Scientist, National Computer Security Center..*



Bruce Schneier: Five Truisms

1. On internet, attack easier than defense.
2. Most software is poorly written and insecure.
3. Connecting everything to each other via the internet will expose new vulnerabilities.
4. Everybody has to stop the best attackers in the world.
5. Laws inhibit security research.

https://www.schneier.com/blog/archives/2017/02/security_and_th.html

Current State of Computer Security

- Computer security today is in bad shape:
  - People worry about it a lot
  - Spend a good deal of money
  - Most systems remain insecure.

-- Butler Lampson

Former PARC Director

parc® Palo Alto Research Center

Security: Physical and Digital

Physical Security: Mature. Well established.

Cyber Security: relatively new. Arguably not well established.

- 1970, new security issues surfaced, OpsSec created
- 1980, more new security issues, CompSec created
- 1990, still more new security issues, CommSec created
- 2000, still, still more new security issues, Information Assurance created
- 2010, yet more new security issues, Homeland Security created
- 2014, NIST Framework for Improving Critical Infrastructure Cybersecurity created…

Anyone see a pattern?

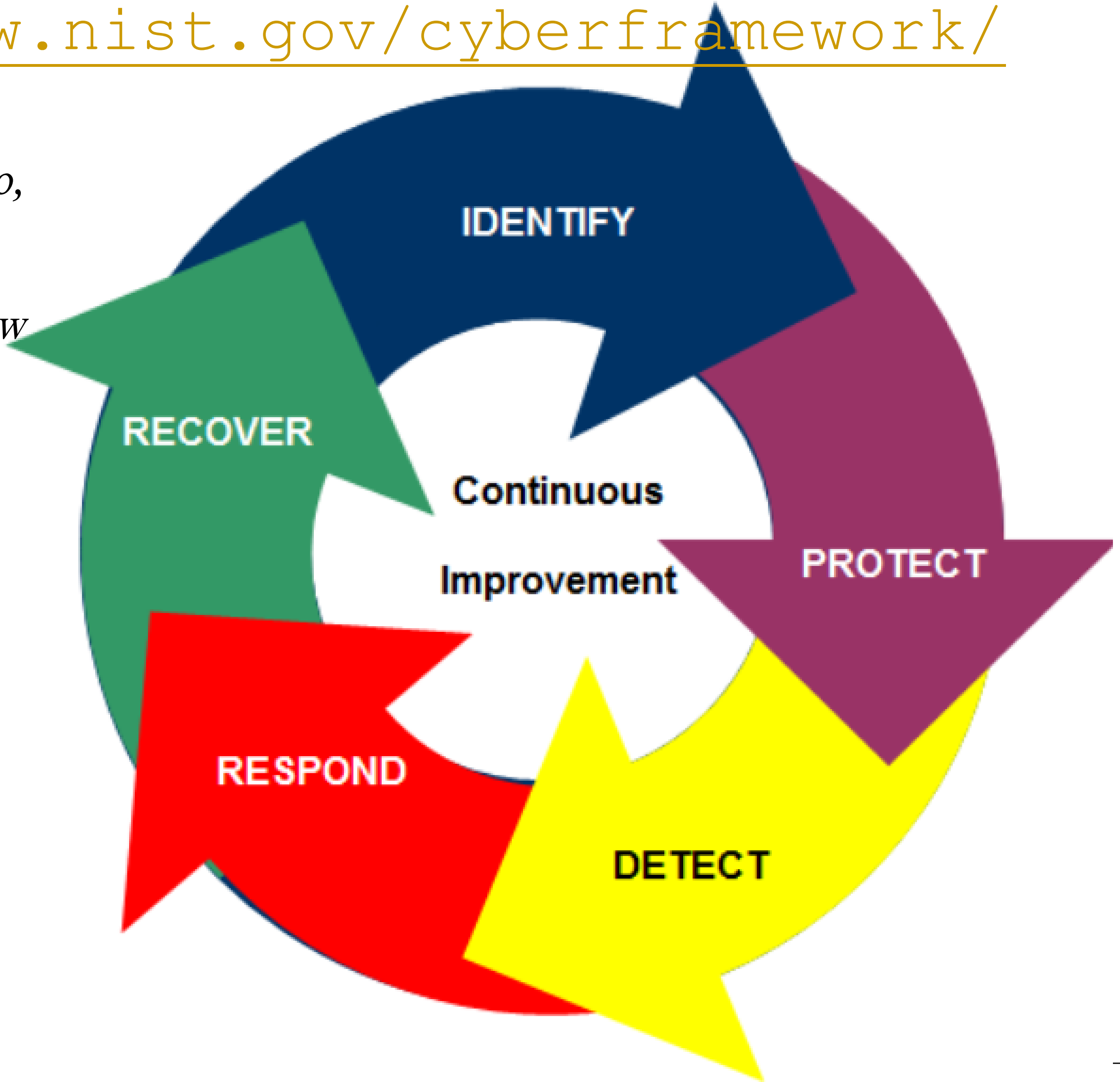
Anyone think that the above represents a solution?

National Institute of Standards and Technology
U.S. Department of Commerce

Cyber Security Framework 2014

http://www.nist.gov/cyberframework/

Forty six years ago, every Sentry Dog Team already knew this…



Bruce Schneier

Two Basic Security Paradigms

1. We either try to secure something well the first time, or
2. We make our security agile.

- First paradigm is security for a world where getting it right is paramount because getting it wrong means people dying.
- Second paradigm comes from the fast-moving and heretofore largely benign world of software.
  - Here, we stress survivability, recoverability, mitigation, adaptability, and muddling through.
  - Security for a world where getting it wrong is okay, as long as you can respond fast enough.

- In the IoT, these two worlds are colliding.

Sentry Dog Security

1. Knowing your assets, vulnerabilities, and threats) is critical. (*Security awareness*.)
2. Effective security requires constant education and training.
3. Longer intrusion undetected, greater the damage.
4. Effective response requires planning, analysis, mitigation, and deterrence.
5. Recovery plans always necessary.

Physical Security

- Top Dog launched two days after a successful Viet Cong attack on Da Nang AB (1 July65) . [1.]
  - Placed sentry dog teams on perimeter in front of machine gun towers/bunkers.
  - Sentry dog teams mission: detection and warning.
    - Alerts followed by rapid response.
    - Proved successful…

Viet Cong learned to fear working dogs.

- Placed a bounty on all dog teams.
  - Higher bounty on dog than handler.
- No undetected attack ever occurred on any US base defended by sentry dogs.

If we can do physical security well, why so many problems with computer security?

1. http://www.usafpolice.org/k-9-in-se-asia.html

Butler Lampson

- Users don’t understand security or security models.
  - The costs either of getting security or of not having it are not known so users don’t care…

Professor Crowley

  - Many, many c-level executives don’t understand either. Consequently, they also don’t care…
  - Modern humans don’t have an effective computer security model consequently they don’t even know enough to care.
- Current legal environment often makes it cheaper to deal with a security breach than to have good security.
- Do security vendors care?

ADE 651 fake bomb detector

Sold to 20 countries in the Middle East and Far East, including Iraq and Afghanistan, for as much as $60,000 per unit.

The Iraqi government is said to have spent £52 million ($85 million) on the devices.

http://en.wikipedia.org/wiki/ADE_651

Security Vendors

- Would a vendor make a security product that makes people feel secure rather than actually be secure?

https://www.youtube.com/watch?v=yoxo_BQ91bY

?

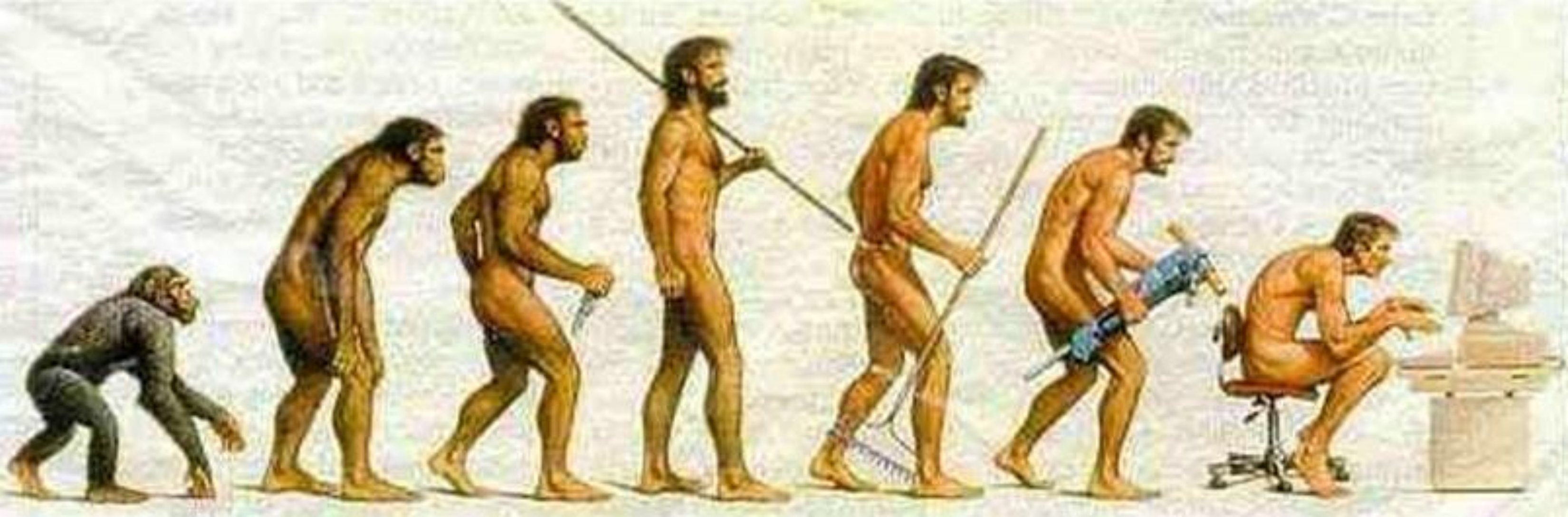
- What happens when a government decides to make people feel more secure rather than actually be more secure?

Security Theater

- Situation where actions are taken to make people feel secure without making them more secure.

http://www.youtube.com/watch?v=GC5NBGx00H4&feature=BF&list=PL5E19028F267592B8&index=1

- If people don't understand security, how can they know when they have more of it?



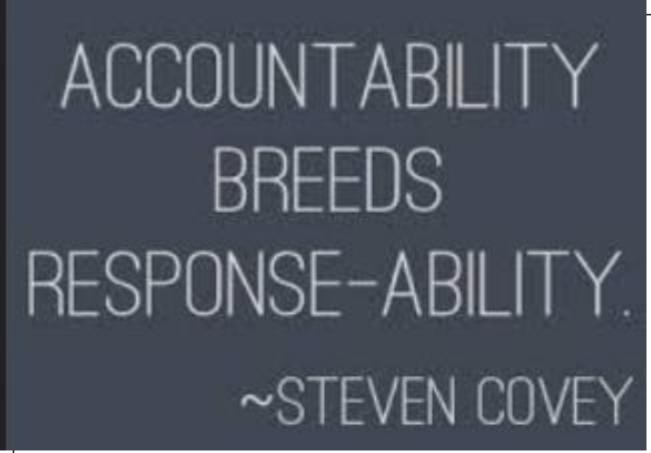
- Daily, humans make security tradeoffs.
- You might think that humans would be good at information security tradeoffs….
- But, you would be wrong.

Why?

- Because, without appropriate training, humans respond to the feeling rather than the reality of security.
- That is, human security model stuck in cave man era.

Security and Deterrence

- People that think that physical security is based on locks are wrong.
  - Locks don’t protect your house from a burglar.
    - Locks slow burglars down.
- What protects your house is deterrence.
  - While the chance of a burglar getting caught may be small, punishment is significant.
  - Consequently, for the most part, burglary is deterred.



ACCOUNTABILITY
BREEDS
RESPONSE-ABILITY.
~STEVEN COVEY

Accountability and the Internet?

- On the Internet, do we have accountability?
  - Without accountability, is deterrence possible?
- Do we have the ability to attribute a 'cyber attack' to a particular entity?
- Do we even have a commonly accepted definition of "Cyber Attack?"

From the OECD's "Reducing Systemic Cybersecurity Risk" by Peter Sommer.

www.oecd.org/dataoecd/57/44/46889922.pdf
(PDF Format)

CIA Uses Computer Code To Hide The Origins

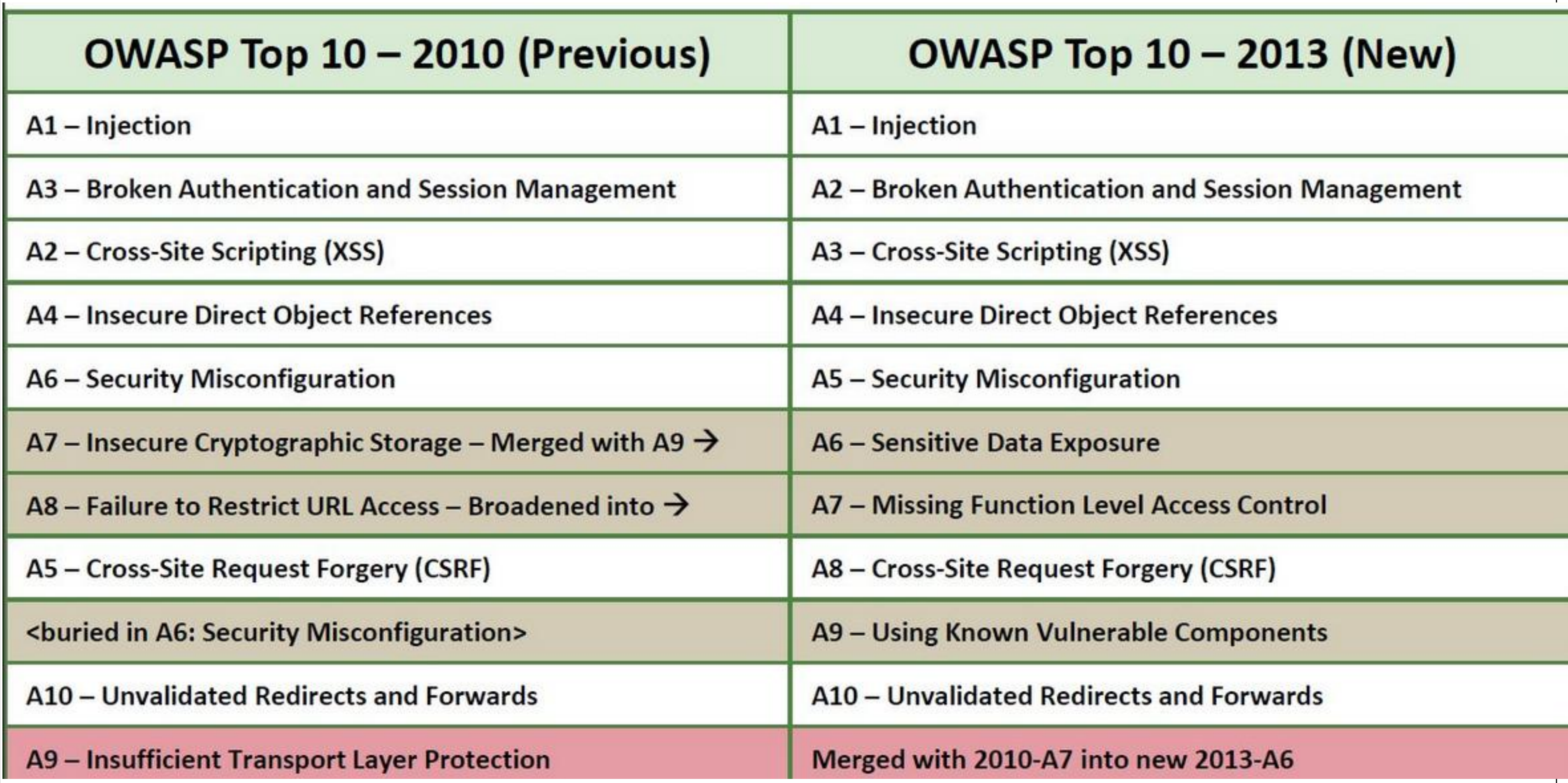
- WikiLeaks shows how CIA's built its hacking attacks in 'disguise … as Russian or Chinese activity'
- WikiLeaks has published hundreds of files which it claims show the CIA went to great lengths to disguise its own hacking attacks and point the finger at Russia, China, North Korea and Iran.
  - WikiLeaks says the source code … has test examples in Chinese, Russian, Korean, Arabic and Farsi .

http://www.dailymail.co.uk/news/article-4367746/WikiLeaks-says-CIA-disguised-hacking-Russian-activity.html#ixzz4ecsUzyFk

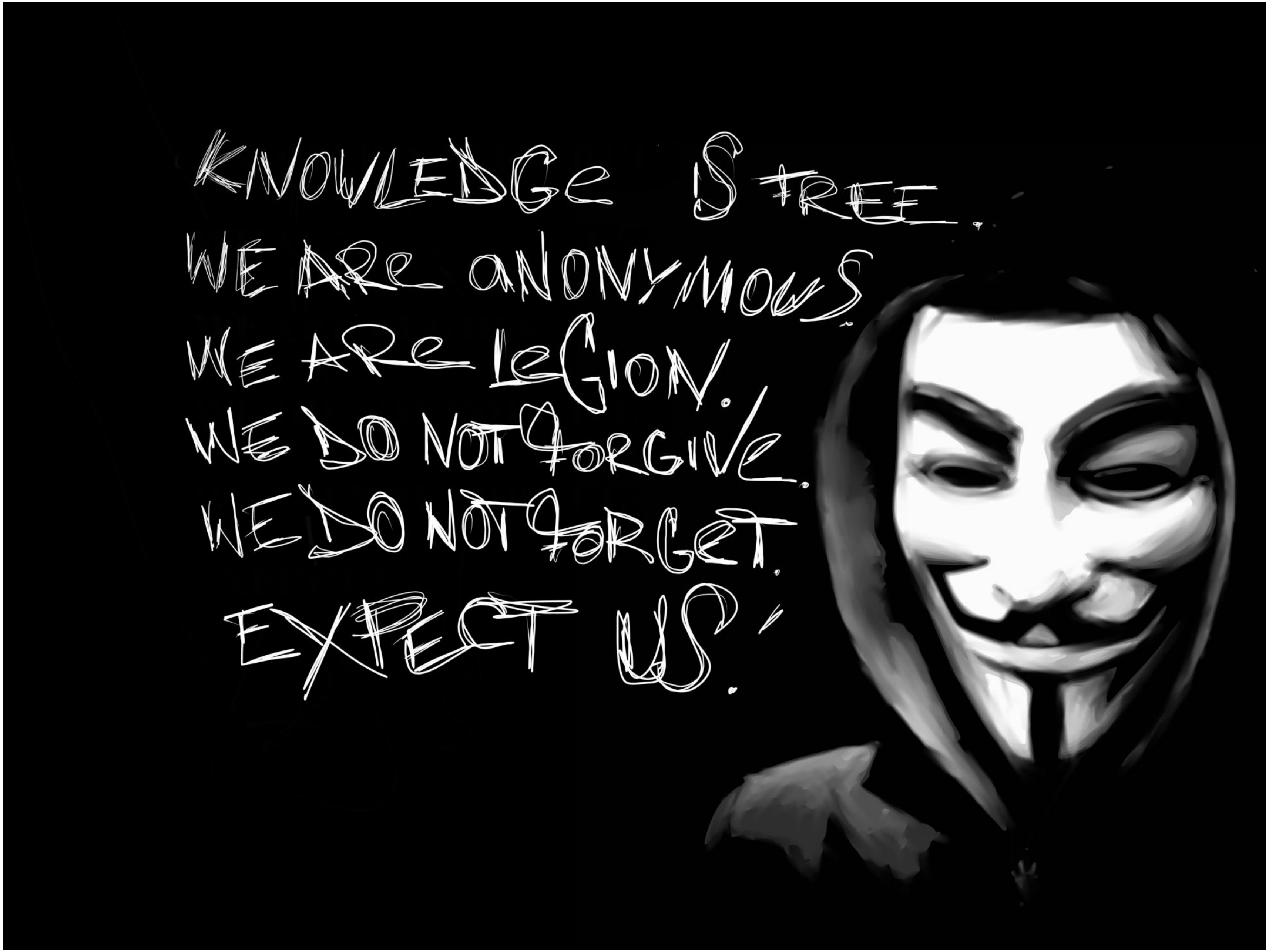
- In the end, though, attribution comes down to whom you believe.

https://www.schneier.com/blog/archives/2017/01/attributing_the_1.html

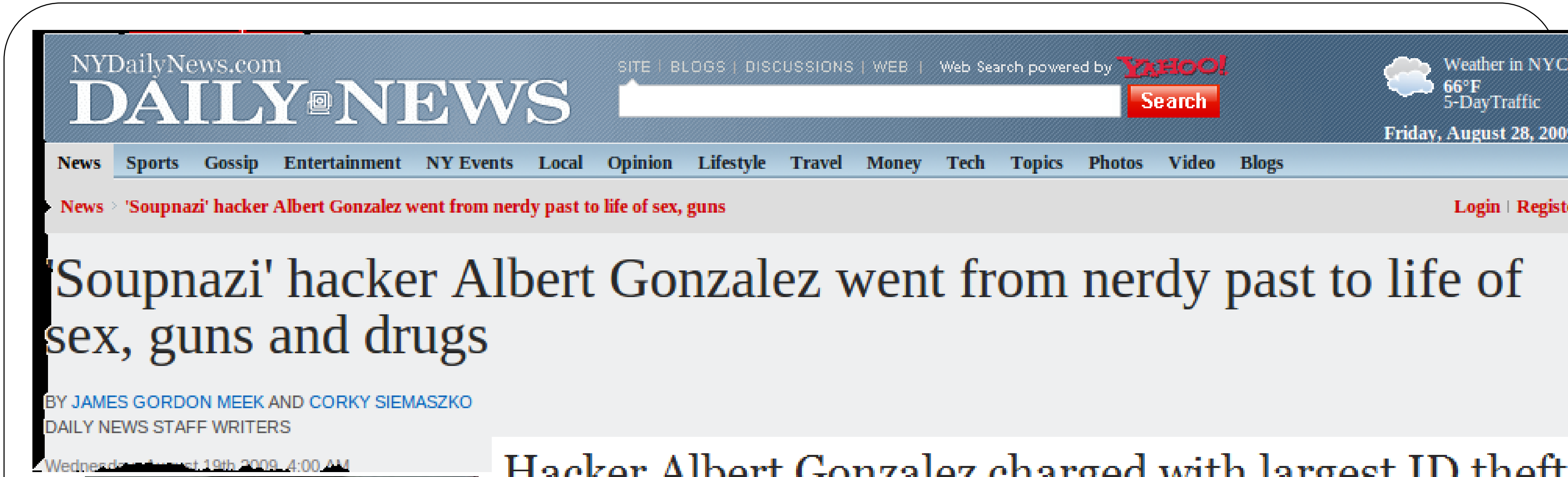
OWASP Top Ten Security Risks



OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6



http://www.youtube.com/watch?v=ny1vT9A9RBc



'Soupnazi' hacker Albert Gonzalez went from nerdy past to life of sex, guns and drugs

BY JAMES GORDON MEEK AND CORKY SIEMASZKO
DAILY NEWS STAFF WRITERS

Wednesday, August 19th 2009, 4:00 AM

Hacker Albert Gonzalez charged with largest ID theft ever involving 130M credit, debit cards

BY JAMES GORDON MEEK
DAILY NEWS WASHINGTON BUREAU

Monday, August 17, 2009

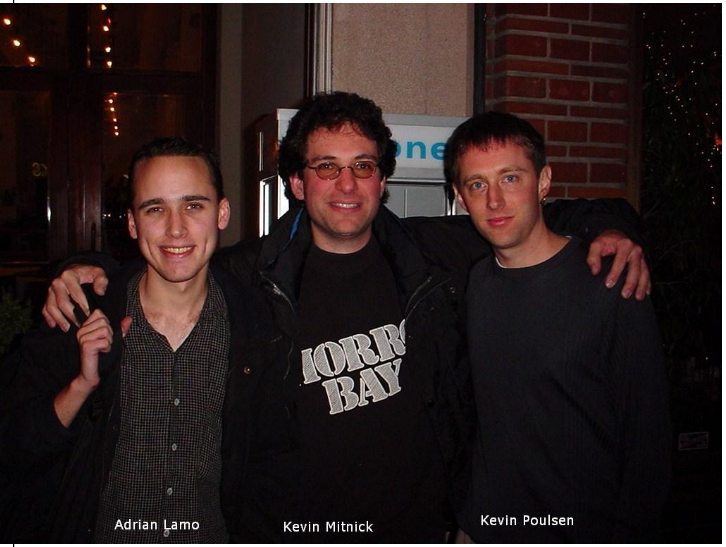
A computer hacker known as "Soupnazi" swiped more than 135 million credit and debit card numbers from top chains like 7-Eleven - the largest theft ever of its kind, prosecutors charged yesterday.

Albert Gonzalez, 28, of Miami, apparently broke his own previous eye-popping record of 40 million card numbers stolen from stores such as T.J. Maxx, Barnes & Noble and Boston Market.

Are criminal hackers different than ordinary criminals?

Who benefits from that feeling?

Threats Examples: Old School

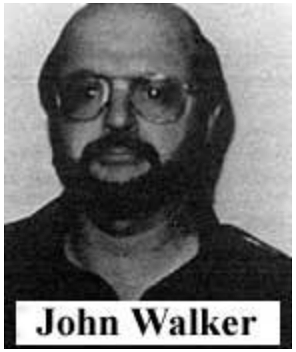


Adrian Lamo
Kevin Mitnick
Kevin Poulsen

Alexey Ivanov
Vasiliy Gorshkov

Max Butler

Robert
Hanssen



John Walker

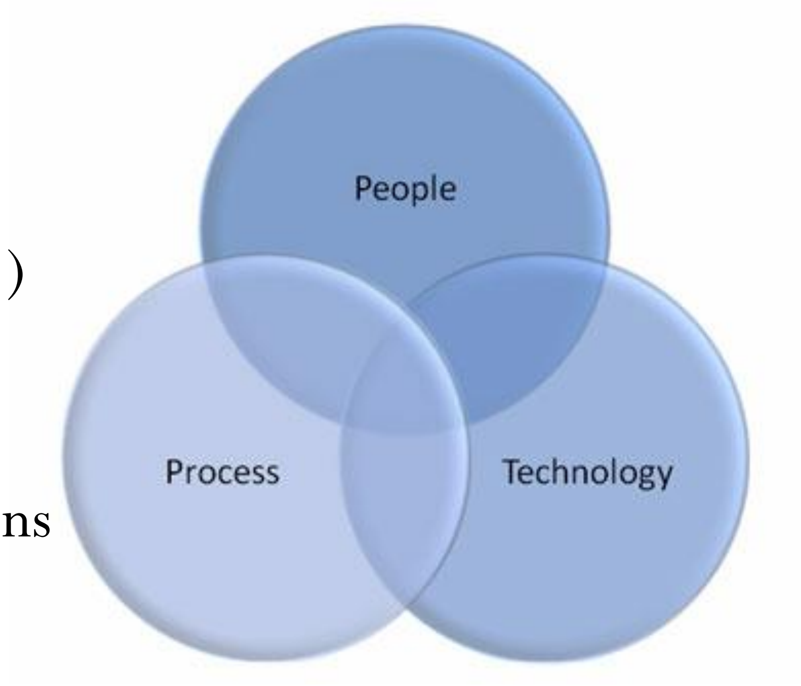
Gary McKinnon

The computer hacker known as "Mafiaboy," who crippled several major Internet sites, arrives in court Thursday in Montreal, Canada

Mafia Boy

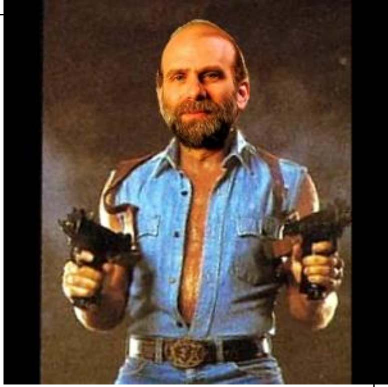
Vulnerabilities Everywhere!!!

- People
  - Lack of situational awareness
  - Social engineering
  - Insiders (bribes, incompetence…)
- Processes
  - Online Financial Transactions
  - Conventional Financial Transactions
  - Credit, debit, and ATM cards
- Technology
  - Computer and Communications Systems
  - Point of sale terminals
  - VA databases, etc…
- Vulnerabilities are Dynamic
- Typically, people considered weakest link.



Any organization can be modeled using a PPT model.

Technical Countermeasures



If you think technology can solve your security problems, then:

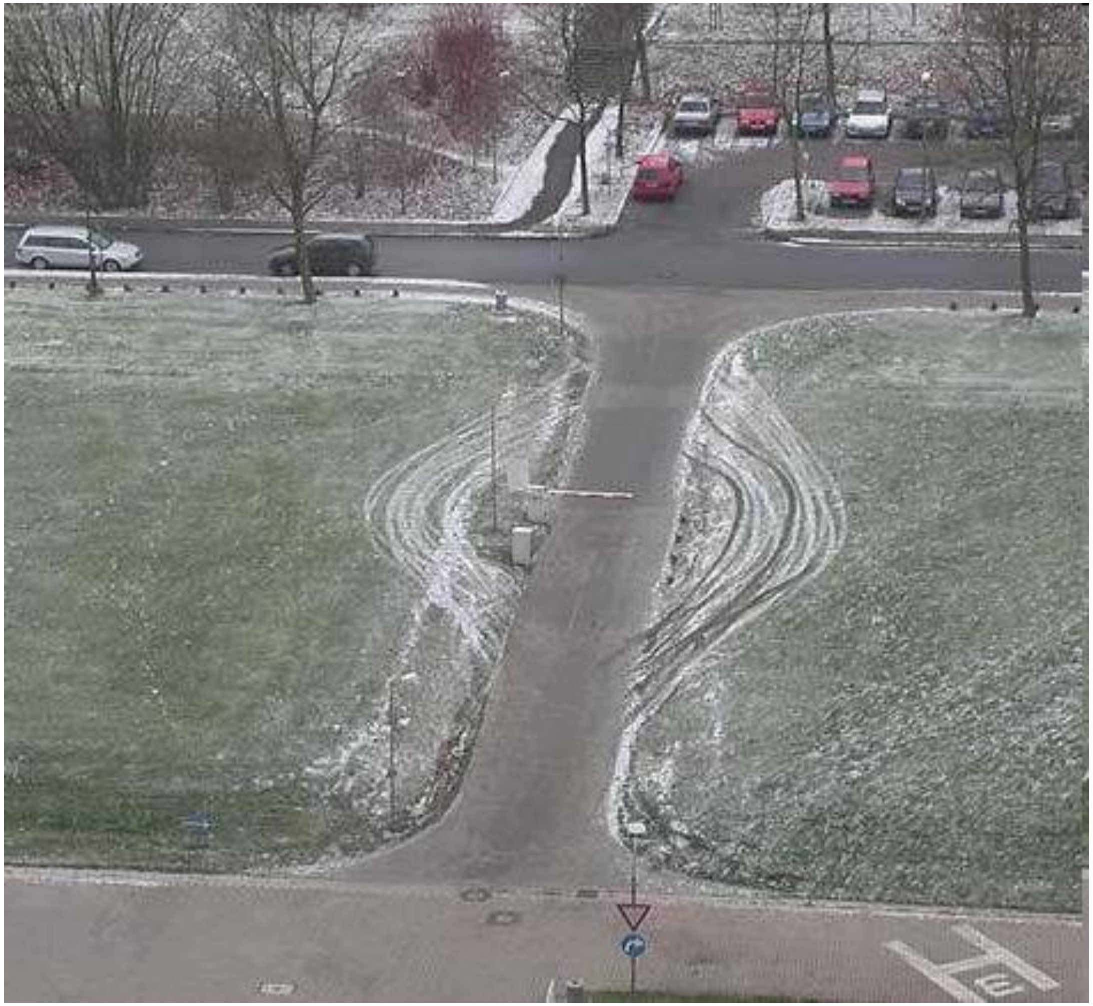
You don't understand the problems

and

You don't understand the technology.

B. Schneier

Technical Countermeasure: An Example



Summary

- To a lay person, feeling secure is indistinguishable from actually being secure.
- Security is hard.
  - Doesn't occur by accident.
- Physical security different than information security.
  - Cybersecurity draws practitioners from a wide variety of fields.
  - Draws many snake oil practioners as well…
- Current environment is rapidly evolving.
- Perfect security not possible.
  - No technological silver bullets!
- Training/Models help with understanding and communicating security.

For Further Study

ISC^2 Common Body of Knowledge

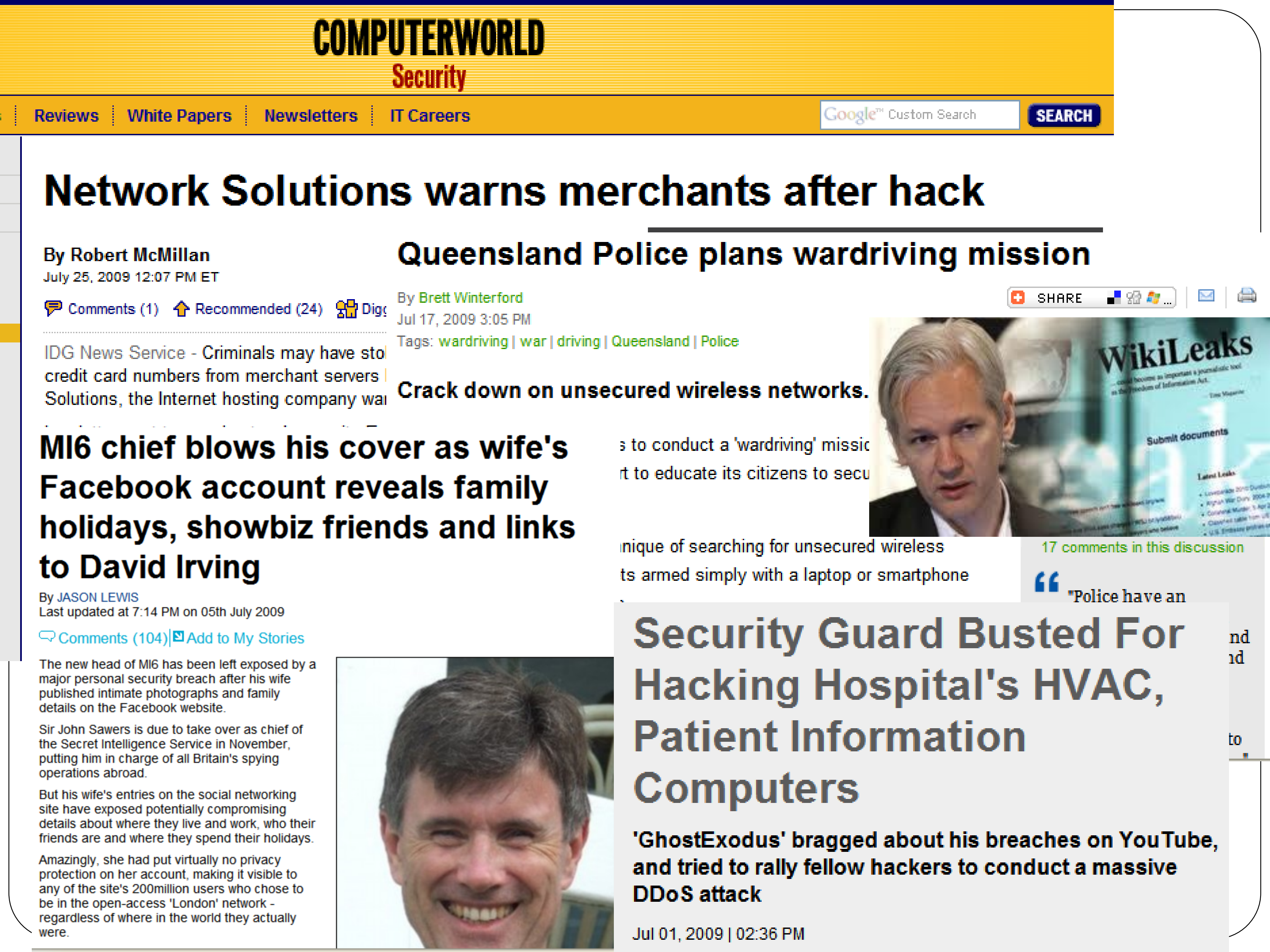
- Access Control
  - Categories and Controls
  - Control Threats and countermeasures
- Application Development Security
  - Software Based Controls
  - Software Development Lifecycle and Principles
- Business Continuity and Disaster Recovery Planning
  - Response and Recovery Plans
  - Restoration Activities
- Cryptography
  - Basic Concepts and Algorithms
  - Cryptography standards and algorithms
  - Signatures and Certification
  - Cryptanalysis
- Information Security Governance and Risk Management
  - Policies, Standards, Guidelines and Procedures
  - Risk Management Tools and Practices
  - Planning and Organization
- Legal, Regulations, Investigations and Compliance
  - Major Legal Systems
  - Common and Civil Law
  - Regulations, Laws and Information Security
- Operations Security
  - Media, Backups and Change Control Management
  - Controls Categories
- Physical (Environmental) Security
  - Layered Physical Defense and Entry Points
  - Site Location Principles
- Security Architecture and Design
  - Principles and Benefits
  - Trusted Systems and Computing Base
  - System and Enterprise Architecture
- Telecommunications and Network Security
  - Network Security Concepts and Risks
  - Business Goals and Network Security

Questions???

Thanks for listening!

Stay safe! Ed Crowley

--following are some slides that used to be part of this presentation. But I may add them into future presentations….



Network Solutions warns merchants after hack

By Robert McMillan
July 25, 2009 12:07 PM ET

IDG News Service - Criminals may have sto
credit card numbers from merchant servers
Solutions, the Internet hosting company wa

Queensland Police plans wardriving mission

By Brett Winterford
Jul 17, 2009 3:05 PM
Tags: wardriving | war | driving | Queensland | Police

Crack down on unsecured wireless networks.

s to conduct a 'wardriving' missic
t to educate its citizens to secu

nique of searching for unsecured wireless
ts armed simply with a laptop or smartphone

17 comments in this discussion

"Police have an

nd
nd

to

MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving

By JASON LEWIS
Last updated at 7:14 PM on 05th July 2009

The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website.

Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain's spying operations abroad.

But his wife's entries on the social networking site have exposed potentially compromising details about where they live and work, who their friends are and where they spend their holidays.

Amazingly, she had put virtually no privacy protection on her account, making it visible to any of the site's 200million users who chose to be in the open-access 'London' network - regardless of where in the world they actually were.

Security Guard Busted For Hacking Hospital's HVAC, Patient Information Computers

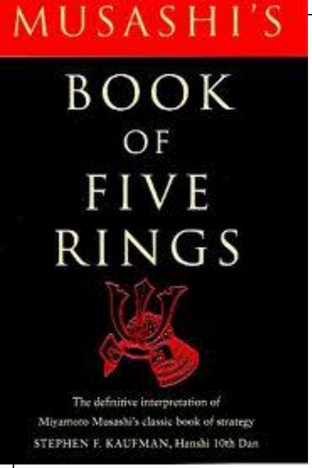
'GhostExodus' bragged about his breaches on YouTube, and tried to rally fellow hackers to conduct a massive DDoS attack

Jul 01, 2009 | 02:36 PM

IN ORDER TO LEARN JUST THAT MUCH,
I WASTED* TWENTY-TWO YEARS.
T/N: THE WORD USED HERE CAN ALSO MEAN "DEVOTED" OR JUST "SPENT"

Your most important weapon is the one between your ears.

(http://www.youtube.com/user/bigredd21) *Miyamoto Musashi Vagabond…*

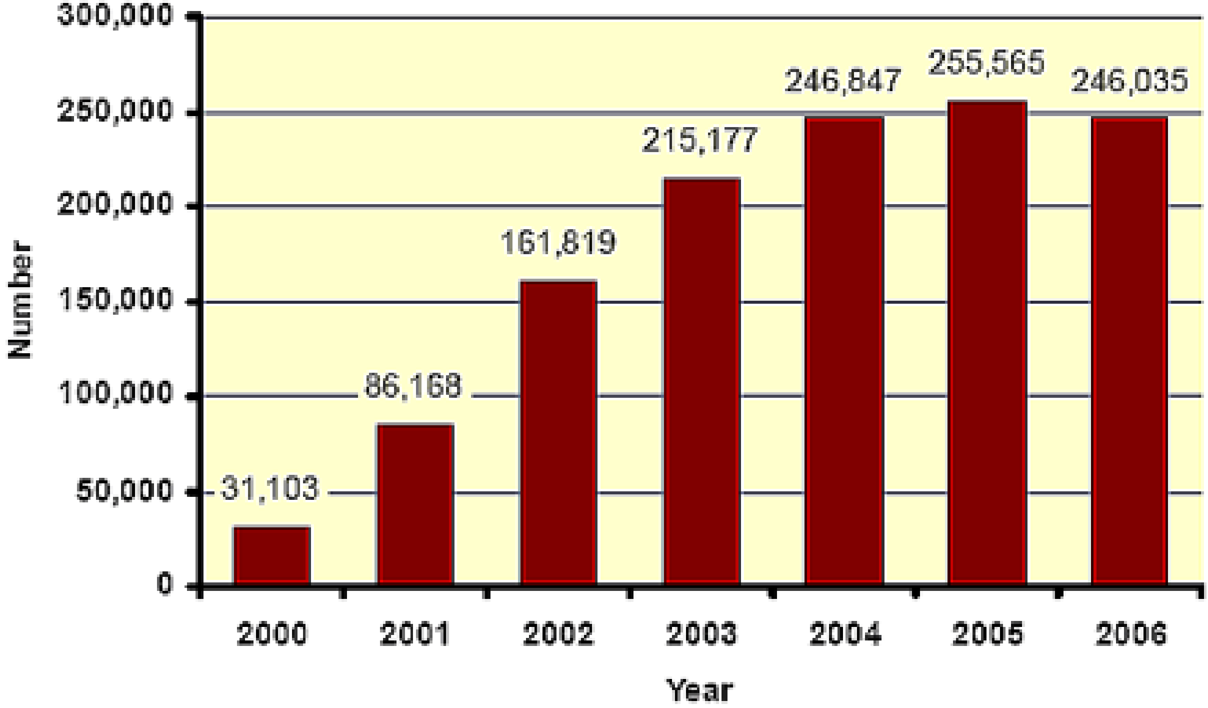

MUSASHI'S
BOOK
OF
FIVE
RINGS
The definitive interpretation of
Miyamoto Musashi's classic book of strategy
STEPHEN F. KAUFMAN, Hanshi 10th Dan

Miyamoto Musashi, Ronin

- Do not intend to rely on anything
- Respect the gods and Buddhas, do not depend on them
- Do not regret things about your own personal life
- Do not lament parting on any road whatsoever
- Do not be fond of material things
- Though you give up your life, do not give up your honor
- Never stray from the Way.

From The Way of Walking Alone by Musashi… (1645)

Identity Theft



http://www2.tbo.com/news/politics/2012/mar/20/tampas-tax-fraud-epidemic-gets-national-scrutiny-ar-382823/

http://www.myfoxtampabay.com/dpp/news/local/hillsborough/tampa-detective-testifies-before-congress-03202012

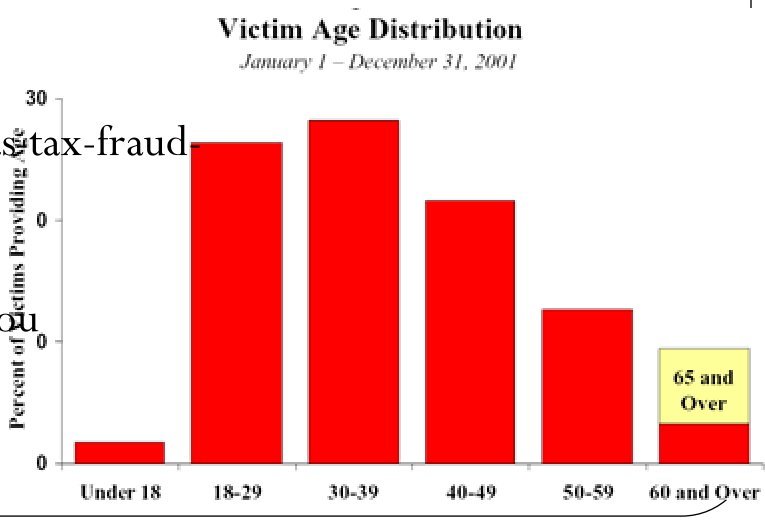
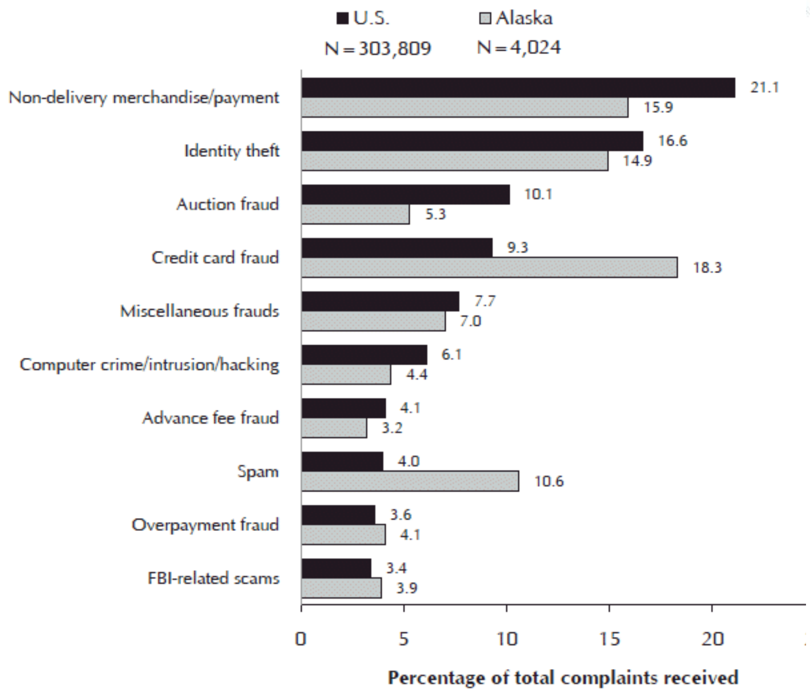
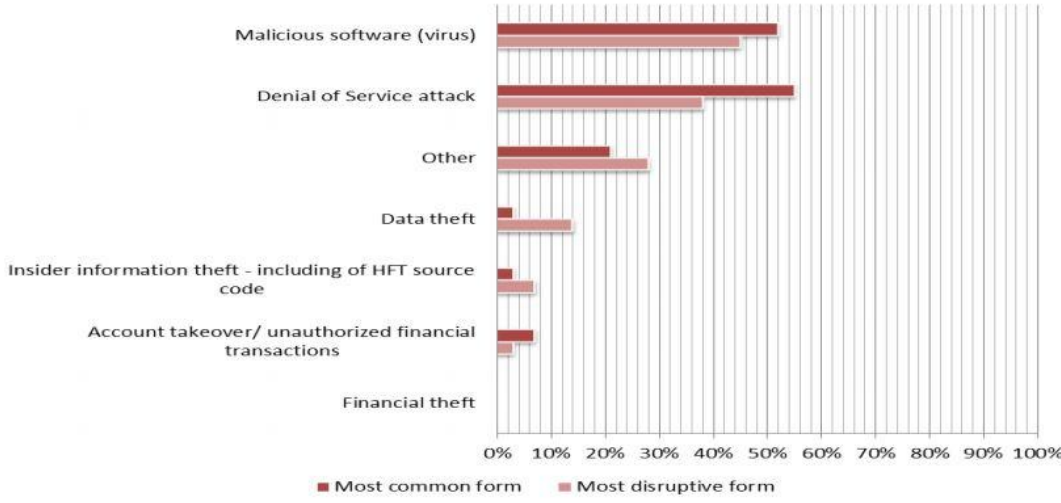


Figure 1. Most Common IC3 Complaint Categories, U.S. and Alaska, 201(



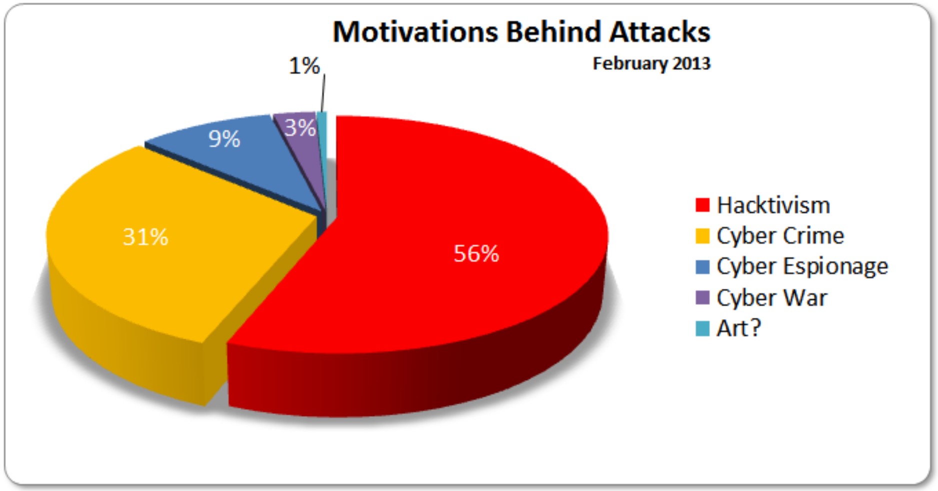
Source of data: *2010 Internet Crime Report, U*

Figure 2: Most common and most disruptive form of cyber-attack?



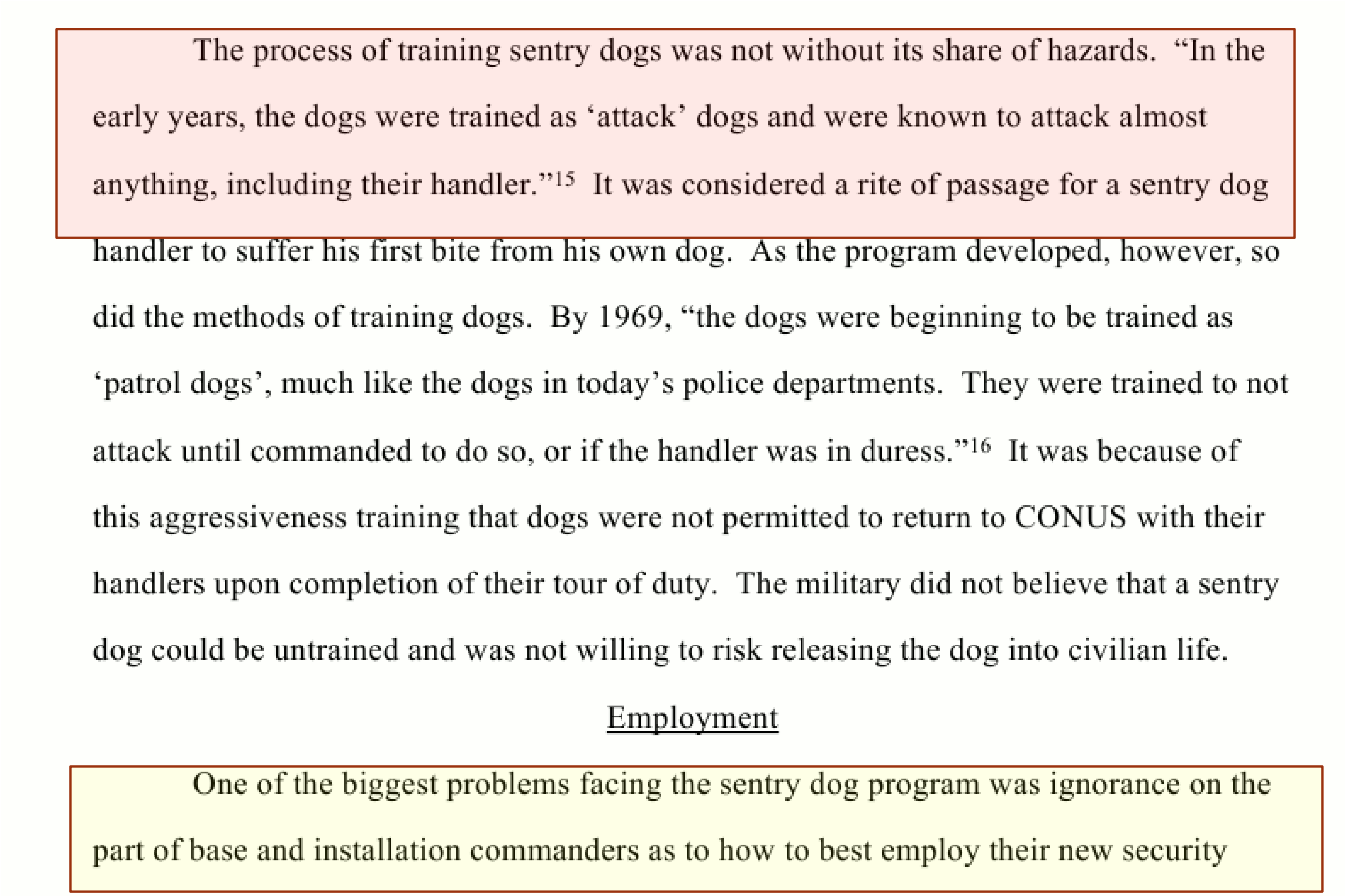
'Other' forms of common attacks reported related to: SQL Injection, Laptop Theft, Website Defacement attempts, Port scanning and spam emails, Phishing email attack, social engineering, Website scanning.

'Other' forms of disruptive threats included: Website defacement attempts, Port scanning and spam emails, Sel replicating email virus, Advanced Persistent threats, infrastructure damaging threats.


Motivations Behind Attacks

February 2013

Training Hazards



The process of training sentry dogs was not without its share of hazards. “In the early years, the dogs were trained as ‘attack’ dogs and were known to attack almost anything, including their handler.”[15] It was considered a rite of passage for a sentry dog handler to suffer his first bite from his own dog. As the program developed, however, so did the methods of training dogs. By 1969, “the dogs were beginning to be trained as ‘patrol dogs’, much like the dogs in today’s police departments. They were trained to not attack until commanded to do so, or if the handler was in duress.”[16] It was because of this aggressiveness training that dogs were not permitted to return to CONUS with their handlers upon completion of their tour of duty. The military did not believe that a sentry dog could be untrained and was not willing to risk releasing the dog into civilian life.

Employment

One of the biggest problems facing the sentry dog program was ignorance on the part of base and installation commanders as to how to best employ their new security

:“The Contributions of the Military Working Dog in Vietnam,” A thesis from the U.S. Army Command and General Staff College by Mary Kathleen Murray, LCDR, USN

Information Security Awareness Why so Elusive?

Consider two different concepts that map to the same word (Security)

1. Feeling
2. Reality

These qualities are separate and distinct.

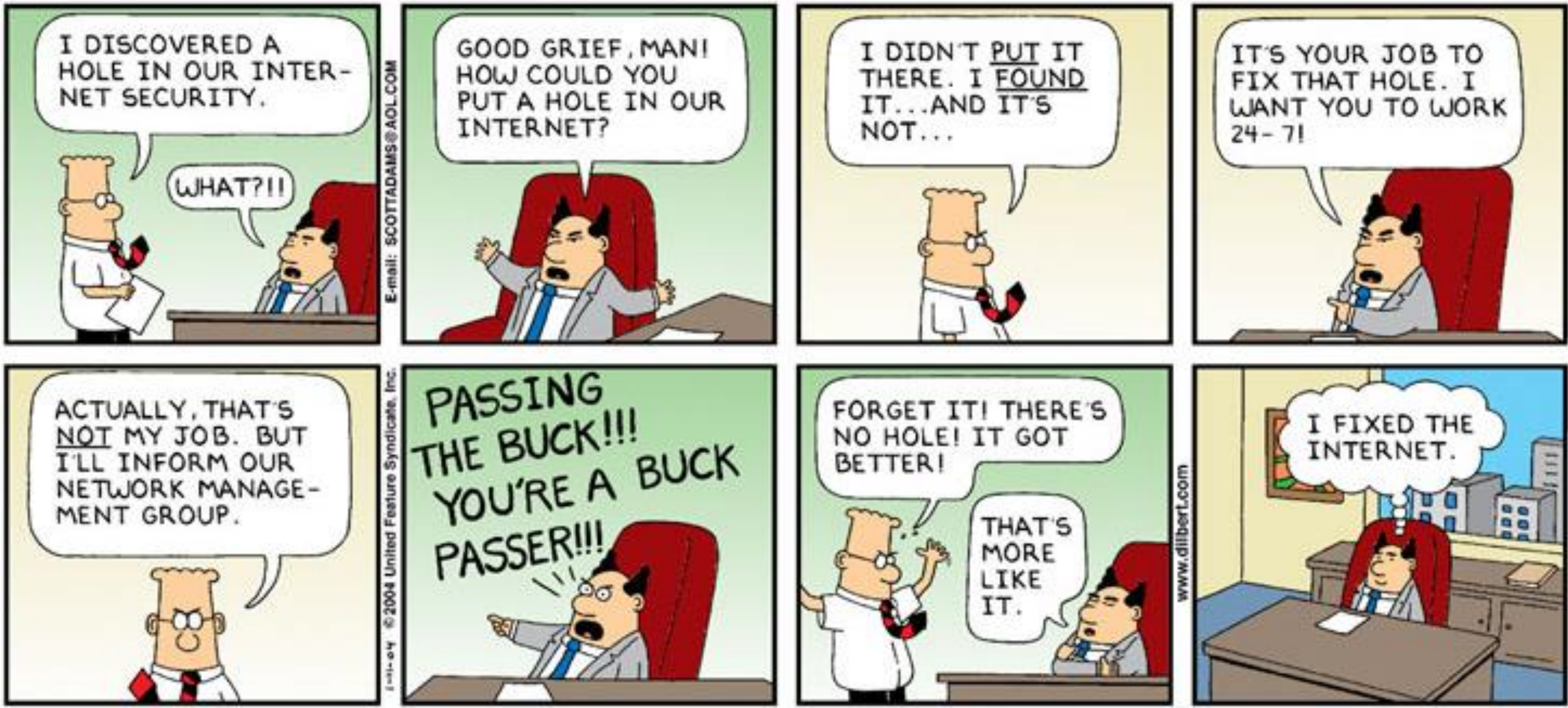
- In addition, many terms have vague or poorly understood definitions.

These two different qualities create four possible states.

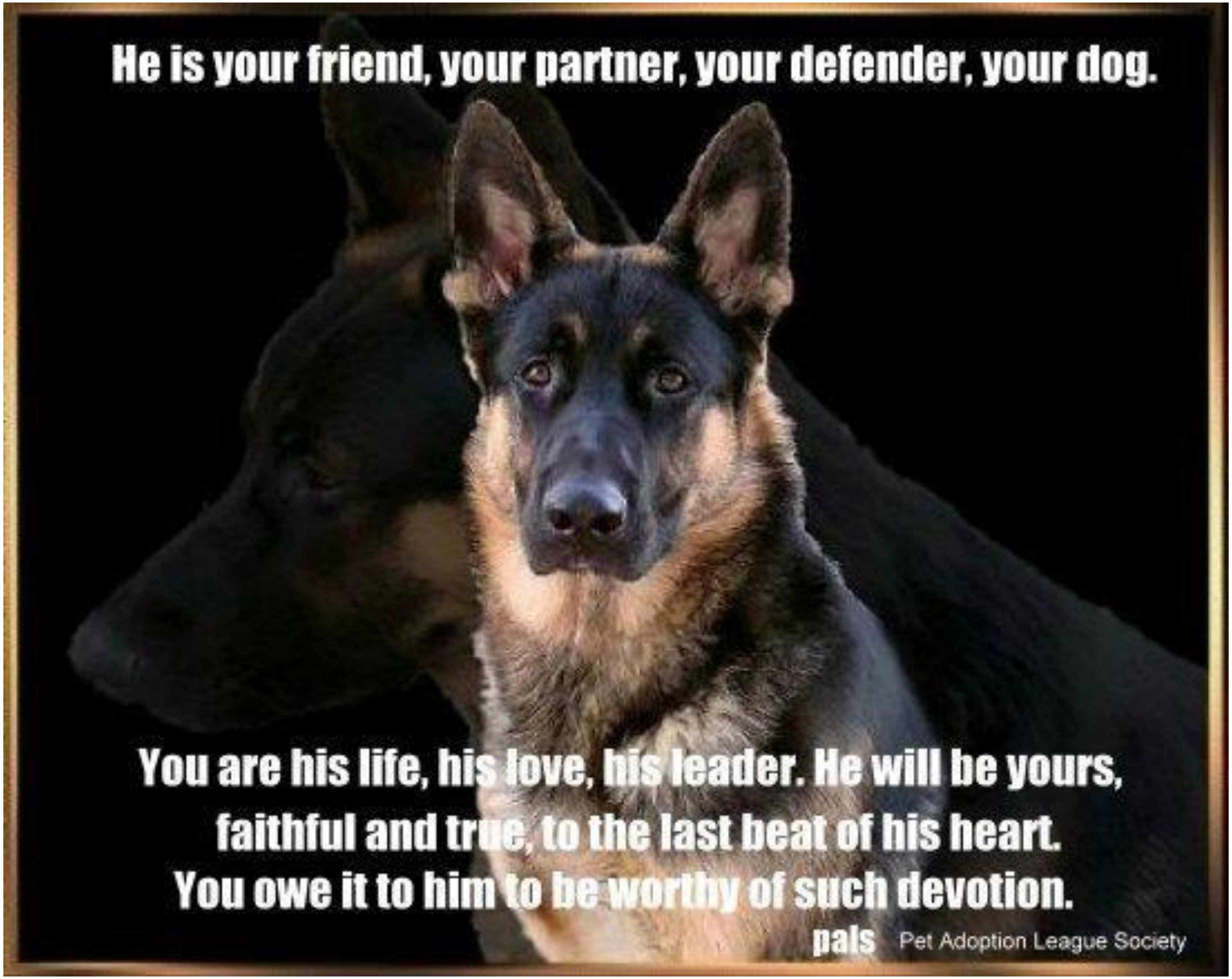
Four Possible Security States

	Think that you are Secure	Think that you are Insecure
Be Secure	Real Security	Illusion
Be Insecure	Illusion	Real Insecurity

Security States Illustrated


I DISCOVERED A HOLE IN OUR INTERNET SECURITY.
WHAT?!!
E-mail: SCOTTADAMS@AOL.COM
GOOD GRIEF, MAN! HOW COULD YOU PUT A HOLE IN OUR INTERNET?
I DIDN'T PUT IT THERE. I FOUND IT...AND IT'S NOT...
IT'S YOUR JOB TO FIX THAT HOLE. I WANT YOU TO WORK 24-7!
ACTUALLY, THAT'S NOT MY JOB. BUT I'LL INFORM OUR NETWORK MANAGEMENT GROUP.
© 2004 United Feature Syndicate, Inc.
PASSING THE BUCK!!! YOU'RE A BUCK PASSER!!!
FORGET IT! THERE'S NO HOLE! IT GOT BETTER!
THAT'S MORE LIKE IT.
www.dilbert.com
I FIXED THE INTERNET.

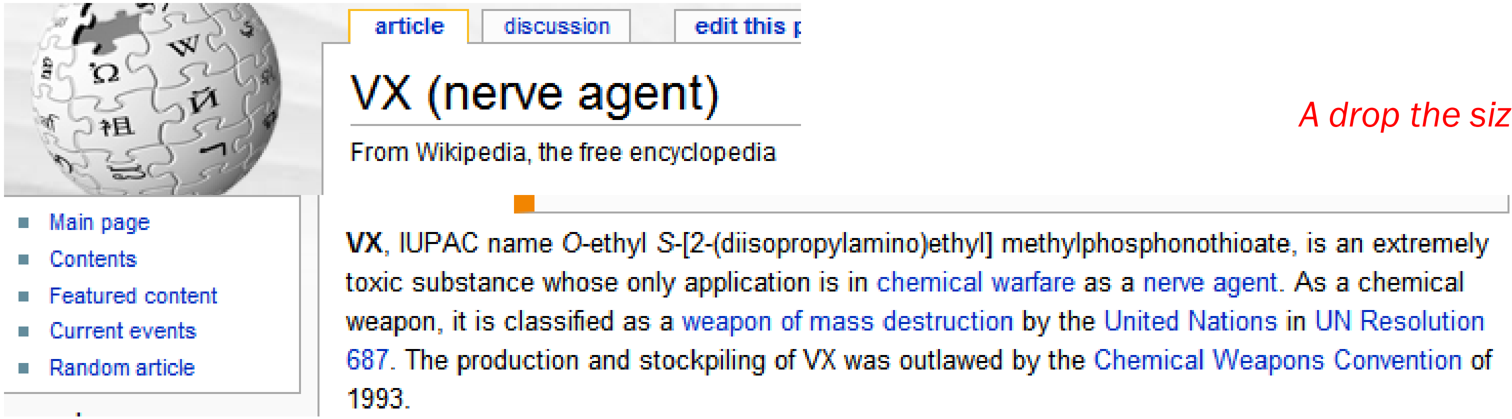
To be secure or to feel secure? That is the question.


He is your friend, your partner, your defender, your dog.
You are his life, his love, his leader. He will be yours, faithful and true, to the last beat of his heart. You owe it to him to be worthy of such devotion.
pals Pet Adoption League Society

Sentry Dogs Remembered： http://cybersd.com/sd/

What did we protect? Nerve Gas

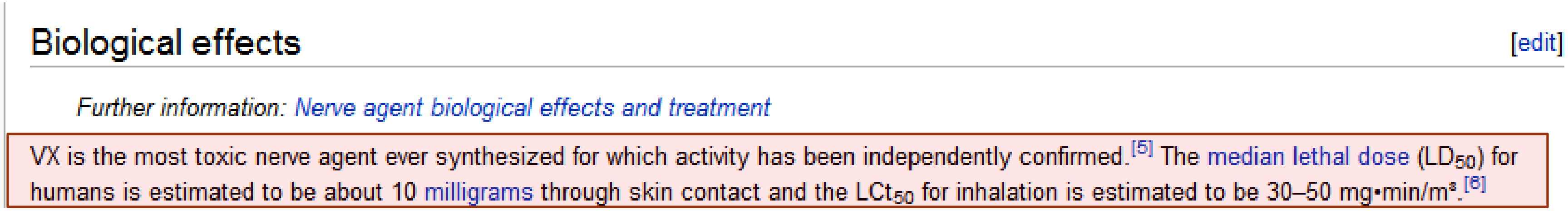
Lethal dose:
A drop the size of Lincoln's eye.



VX (nerve agent)

From Wikipedia, the free encyclopedia

VX, IUPAC name *O*-ethyl *S*-[2-(diisopropylamino)ethyl] methylphosphonothioate, is an extremely toxic substance whose only application is in chemical warfare as a nerve agent. As a chemical weapon, it is classified as a weapon of mass destruction by the United Nations in UN Resolution 687. The production and stockpiling of VX was outlawed by the Chemical Weapons Convention of 1993.



Biological effects

[edit]

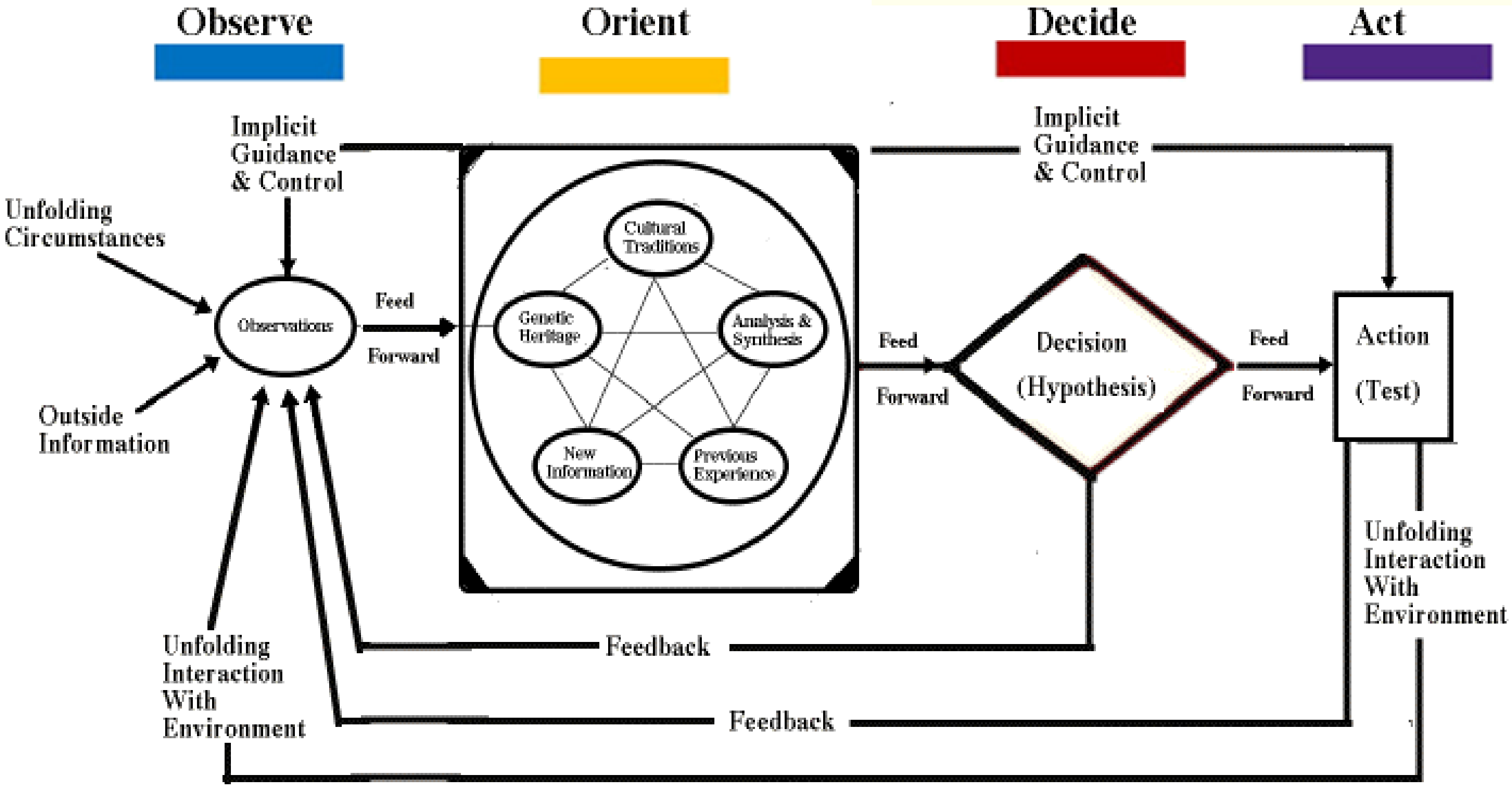
Further information: Nerve agent biological effects and treatment

VX is the most toxic nerve agent ever synthesized for which activity has been independently confirmed.[5] The median lethal dose (LD$_{50}$) for humans is estimated to be about 10 milligrams through skin contact and the LCt$_{50}$ for inhalation is estimated to be 30–50 mg·min/m^3.[6]

NIST Model Overlaid in Colors

Boyd’s OODA Loop

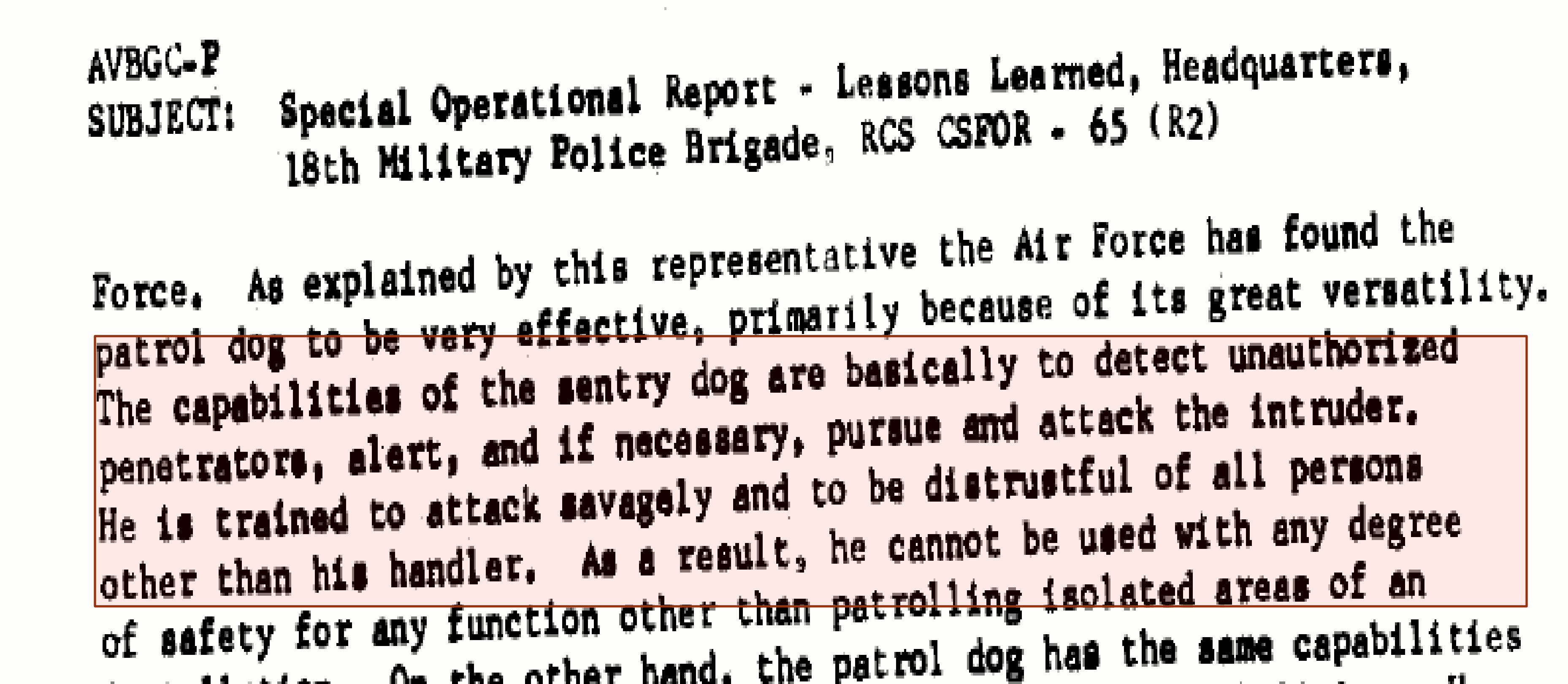
Security Professionals utilize tools (protocol analyzers, intrusion detection systems, and log aggregators) to augment their ability to identify threats. Output from these tools requires analysis (orientation).



John Boyd's OODA Loop

As a Sentry Dog Handler, I observed and analyzed my Dog’s alerts. Greatly increasing my ability to detect and respond to intrusions.

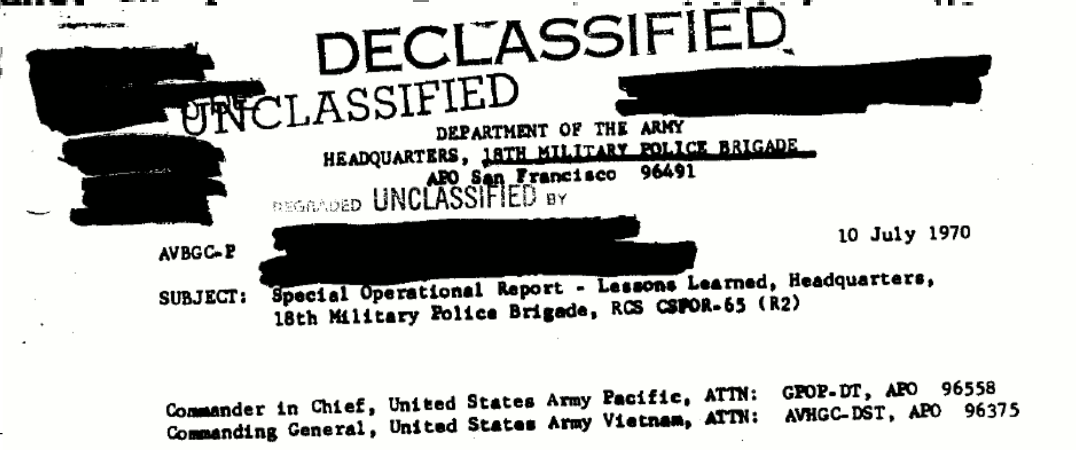
Lessons Learned I



AVBGC-P

SUBJECT: Special Operational Report - Lessons Learned, Headquarters, 18th Military Police Brigade, RCS CSFOR - 65 (R2)

Force. As explained by this representative the Air Force has found the patrol dog to be very effective, primarily because of its great versatility. The capabilities of the sentry dog are basically to detect unauthorized penetrators, alert, and if necessary, pursue and attack the intruder. He is trained to attack savagely and to be distrustful of all persons other than his handler. As a result, he cannot be used with any degree of safety for any function other than patrolling isolated areas of an installation. On the other hand, the patrol dog has the same capabilities as the sentry dog to detect a



[redacted]

DECLASSIFIED

UNCLASSIFIED

[redacted]

DEPARTMENT OF THE ARMY
HEADQUARTERS, 18TH MILITARY POLICE BRIGADE
APO San Francisco 96491

REGRADED UNCLASSIFIED BY [redacted]

AVBGC-P

10 July 1970

SUBJECT: Special Operational Report - Lessons Learned, Headquarters, 18th Military Police Brigade, RCS CSFOR-65 (R2)

Commander in Chief, United States Army Pacific, ATTN: GPOP-DT, APO 96558
Commanding General, United States Army Vietnam, ATTN: AVHGC-DST, APO 96375

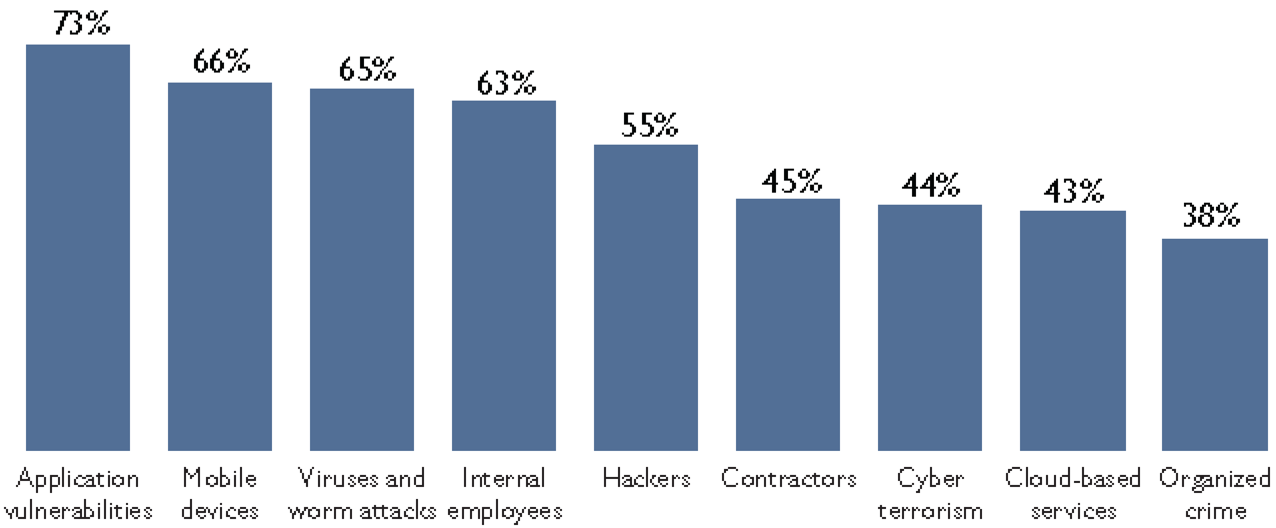
Lessons Learned II

- Poorly led and poorly utilized most security groups are…
  - Cost of security: easy to understand.
  - Cost of a security compromise: difficult to understand
- While security vulnerabilities may be real, feeling secure may be an illusion.
    - Well meaning, or oblivious, insiders can make lethal mistakes.
- Constant improvement i.e. lessons learned are critical.
  - Security environment evolves constantly, if you don’t, you are getting behind.

Selected Threats

- **Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security.** More than 50 percent of information security professionals reported having private clouds in place, and more than 40 percent of respondents reported using software as a service, but more than 70 percent of professionals reported the need for new skills to properly secure cloud-based technologies.

Figure 2—Top Security Threat Concerns



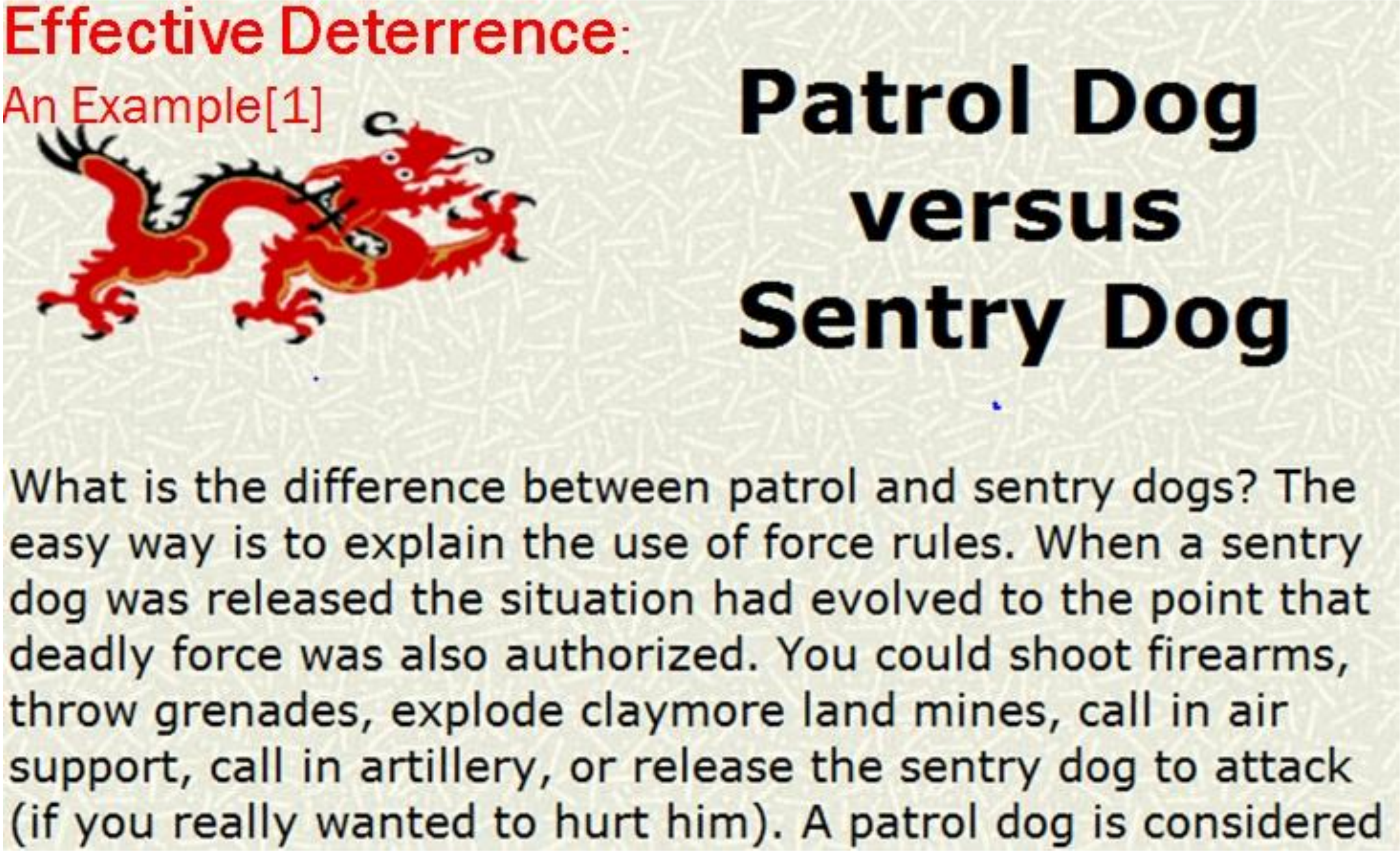
Frost and Sullivan ISC^2 Survey

Security:
Do Humans have a clue?

- What happens when vendors know that humans don't understand?

Risk Management and Security

- With our defined metrics we can measure risk.
    - Threats, Assets, Vulnerabilities
    - The likelihood that a particular threat will find a particular vulnerability…
- Still, what is security? And how can we measure it?
- Can you even prove that you have security?
    - No!
- One factor that makes security unique is that you can't prove that you have it
    - You can only prove that you don't have it
- Security is asymmetric
    - Attackers only have to be successful one time one way…
    - Defenders must be successful each time each way…



Effective Deterrence:

An Example[1]

Patrol Dog versus Sentry Dog

What is the difference between patrol and sentry dogs? The easy way is to explain the use of force rules. When a sentry dog was released the situation had evolved to the point that deadly force was also authorized. You could shoot firearms, throw grenades, explode claymore land mines, call in air support, call in artillery, or release the sentry dog to attack (if you really wanted to hurt him). A patrol dog is considered

Sentry Dog Mission: D^3 “Detect, Detain, Destroy.” [2]

1. http://www.vspa.com/k9/pd-versus-sd.htm
2. http://www.uswardogs.org/war-dog-history/vietnam/