Internet Security and Cyber Crime

… or It's not paranoia if they're ***really*** after you.

Sam Lumpkin

Senior Security Architect

2AB, Inc.

info@2ab.com

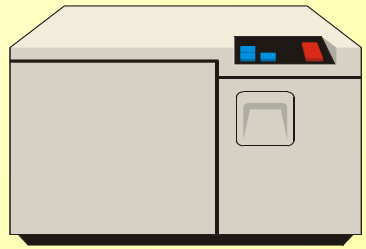
www.2AB.com

Integration Platform For Trusted Solutions

www.2AB.com

WEB AGENT

Authentication



Business Logic

J2EE AGENT

CORBA AGENT

Infrastructure Access Control

Business Logic

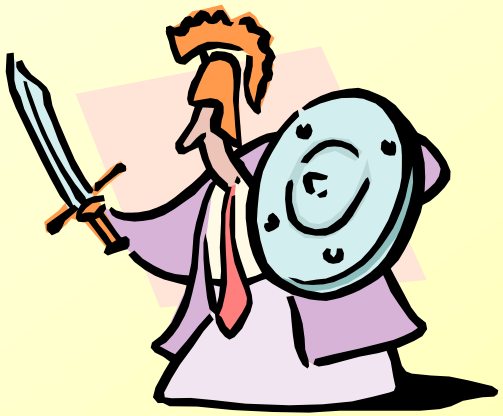
Confidentiality / Message Integrity

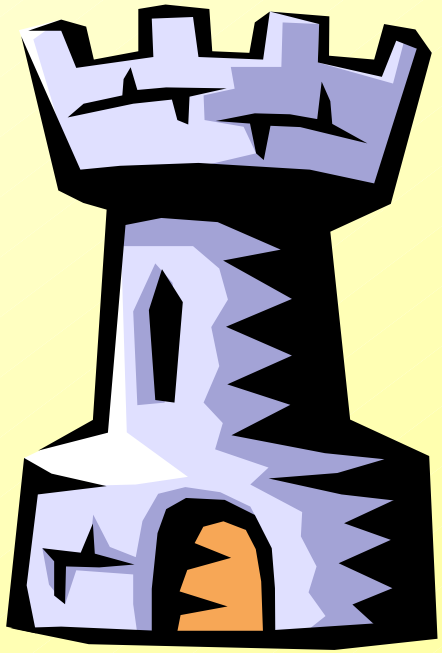
Auditing & Administration

iLOCK

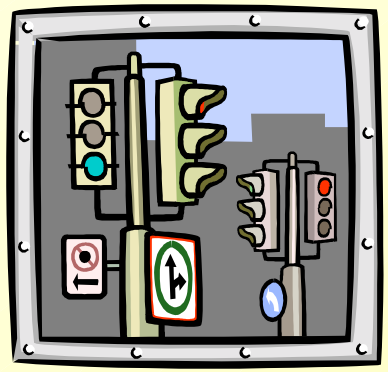
Access Decision, Attribute Mgt, Auditing, Policy Mgt

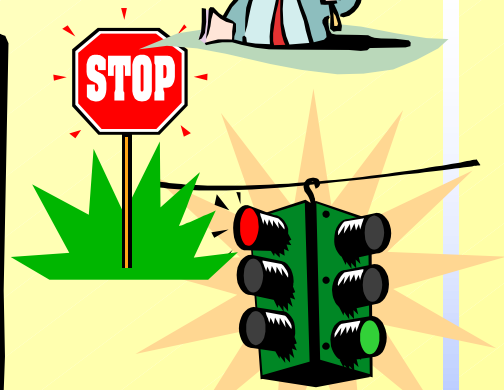
How Management Views Their Company's Security



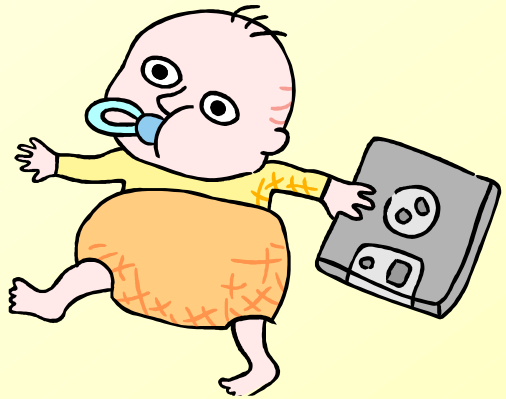


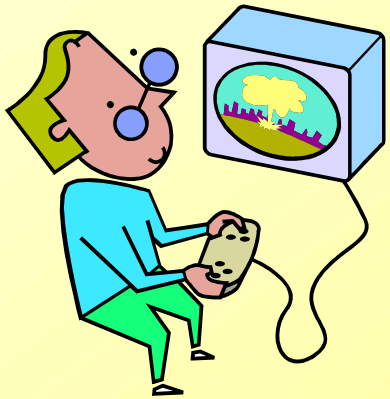
How Internal Users View Their Company's Security

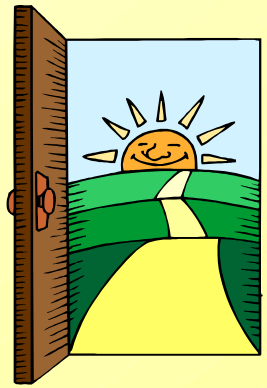




How Crackers and Script Kiddies View a Company's Security

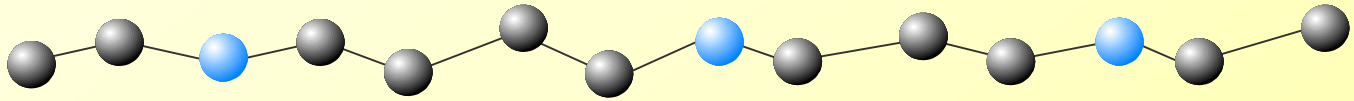






How Bad Can It Be?

Current Headlines

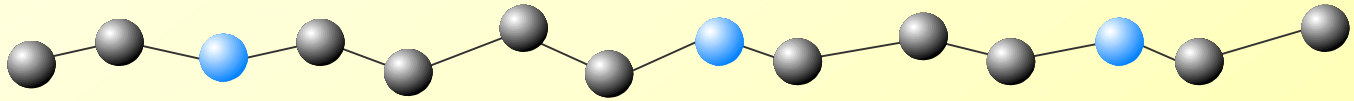


FBI Issues Water Supply Cyberterror Warning

Al-Qaida terrorists have scoured the Web for information on the computerized systems that control water distribution and treatment, NIPC warns.

By Kevin Poulsen, www.securityfocus.com

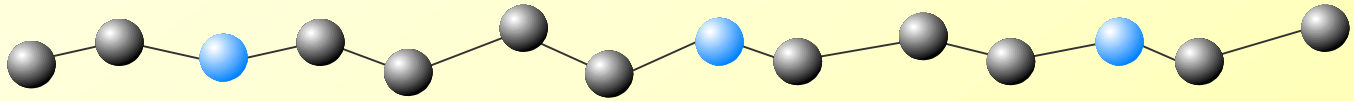
Current Headlines



Microsoft Store Offline After Insecurity Exposed.
By *Brian McWilliams*, Newsbytes
Jan 11 2002 5:52PM PT
An online store operated by Microsoft Corp. [NASDAQ: MSFT] for software developers was unavailable today following reports that a security flaw gave visitors the ability to take control of the site, including access of customer data.

www.securityfocus.com

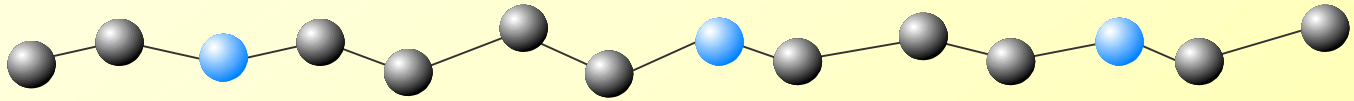
Current Headlines



NASA Hacker Gets 21 Months

Jason 'Shadow Knight' Diekman cracked JPL, Stanford University and others.
By Dick Kelsey, Newsbytes
Feb 5 2002 5:28PM PT
www.securityfocus.com

Headlines

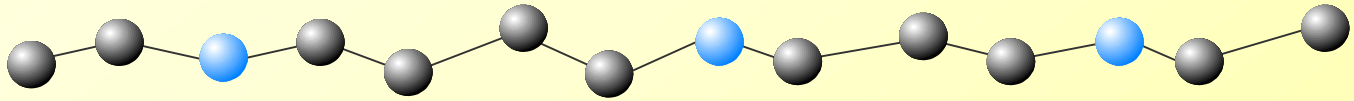


Lloyd's of London To Offer Hacker Insurance

Lloyd's of London, one of world's largest insurance firms, has partnered with San Jose, California-based Counterpane Security, Inc. to offer insurance against business losses due to mischief by hackers.

By Lori Enos E-Commerce Times July 10, 2000

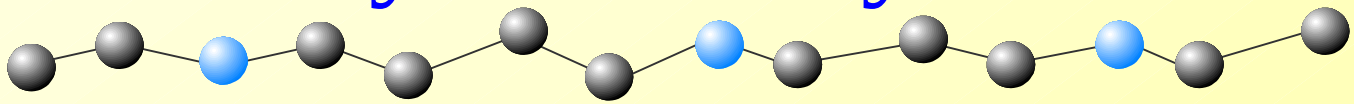
Prediction



Denial of service attacks against companies such as Yahoo! and Amazon.com illustrated the susceptibility of even well-established organizations to hacker attacks. Security incidents had not been widely reported prior to the broadband explosion, however, the Gartner Group predicts that by 2004, service providers will witness a 200 percent increase in the cost of responding to security incidents due to broadband connections.

Pamela Warren, Nortel/Shasta

How common is unauthorized system entry?



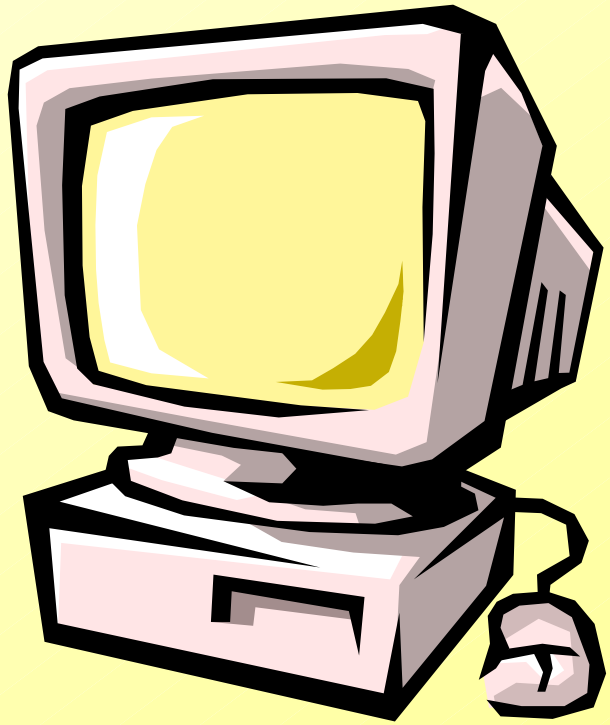
A survey conducted by the Science Applications International Corp. in 1996 found that 40 major corporations reported losing over $800 million to computer break-ins. An FBI survey of 428 government, corporate and university sites found that over 40% reported having been broken into at least once in the last year. One third said that they had been broken into over the Internet. Another survey found that the Pentagon's systems that contain sensitive, but unclassified information, had been accessed via networks illegally 250,000 times and only 150 of the intrusions were detected. The FBI estimates that U.S. businesses loose $138 million every year to hackers. According to the CIA in the past three years government systems have been illegally entered 250,000.

from student paper by Jimmy Sproles and Will Byars for a Computer Ethics Course at ETSU 1998

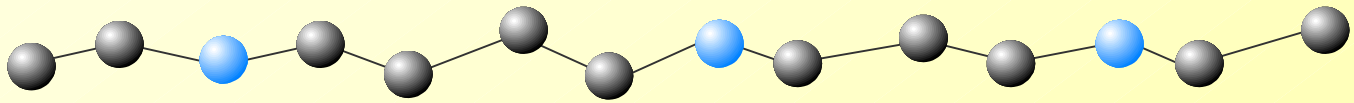
http://www-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm

Point and Click Cracking

- Hacker/Cracker toolkits
- Password crackers
- “Script Kiddies”

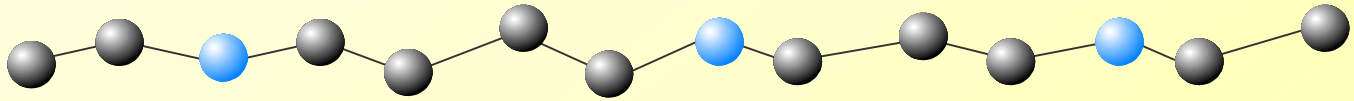


Are “They” in YOUR System?



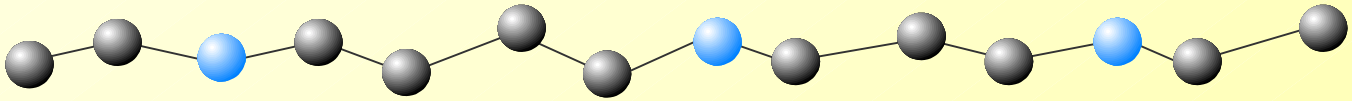
- **Most companies <u>do not know</u>.**
- There is no plan to review logs or scan for unusual activity.
- Physical access is not controlled in a consistent manner.
- If an intrusion were detected or even suspected, there is no procedure designed to deal with it.

Who Are “They”?



- External “They”:
  - “Script Kiddies” (i.e. children)
  - Skilled crackers
  - Foreign nationals (well funded)
  - Competitors or their agents
- Internal “They”:
  - Disgruntled employees
  - Contractors, vendors, temps, etc.

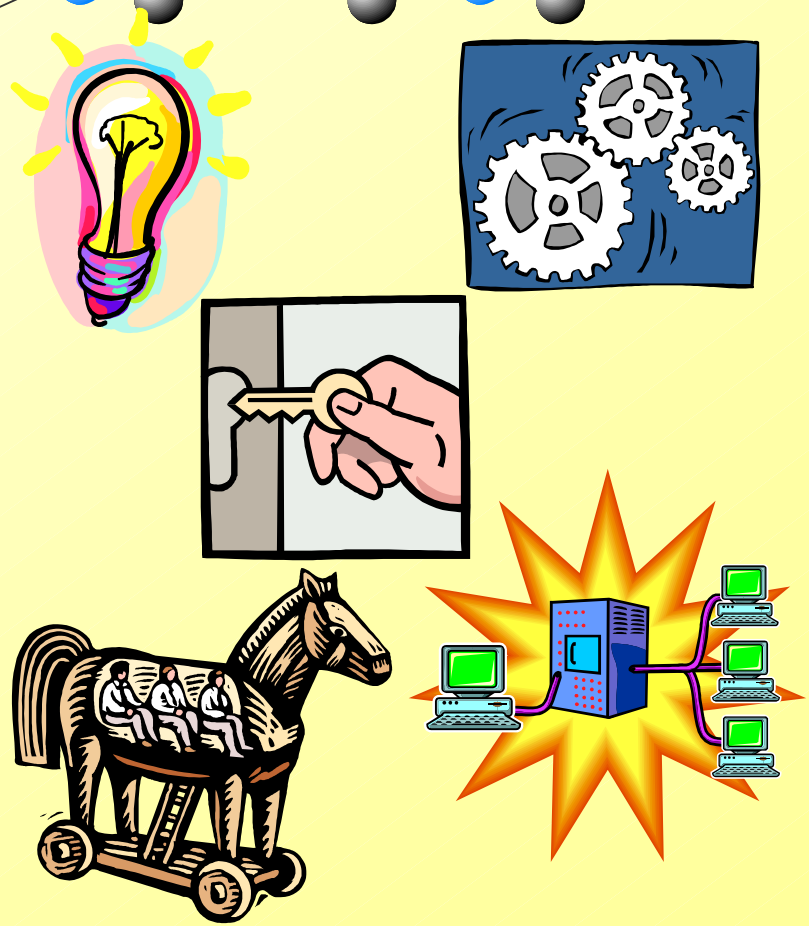
What Can “They” Do?



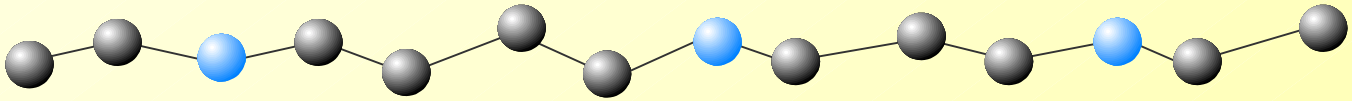
The worst thing “they” can do is to simply quietly gather information and sell it to your competitors, or to other crackers. This can include customer information, trade secrets, payroll information, proposals, and bids. You won’t even know the information has been compromised.

What Else Can “They” Do?

- Destroy data
- Alter data
- Effect any system controlled by computers.
- Imbed Trojan programs for later exploitation.



Why should you care?

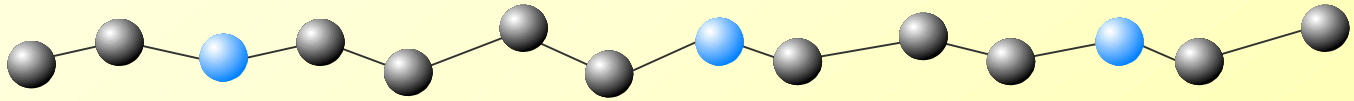


How much is your information worth? What happens if a competitor has access to your pricing, your bids, and your payroll information? How much of you information could you do without and still do business?

With the explosion of on-line services, controlling access to personal information is critical!

The demands of consumers and the requirements of many government regulations such as US Code Title 47 and HIPAA make it mandatory that information be protected.

Why Should You Care?



Corporate Officers And Directors Need To Take Responsibility For Securing Corporate Information Assets, Report Says

Recourse Technologies™ Report, Written by Tech Industry Legal Expert, Finds Evidence That Directors/Officers Can be Held Liable for Loss of Data Due to Hacking.

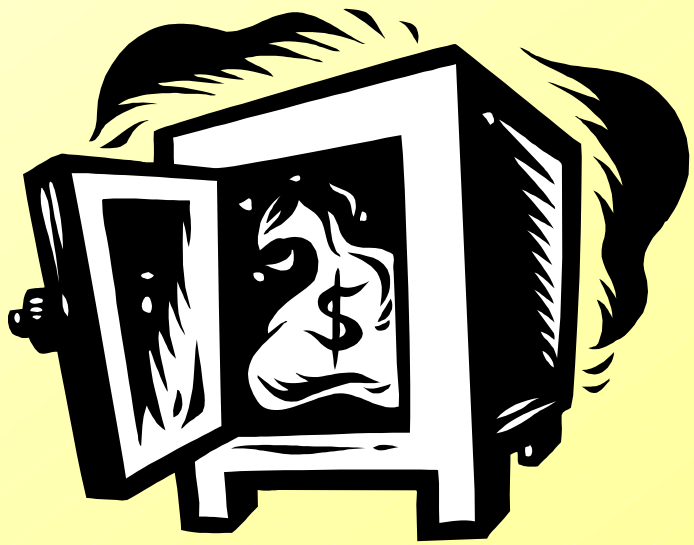
www.recourse.com/download/press/PDF/07.30.01_NOC.pdf

What About Firewalls?

- Firewalls help protect the perimeter of your network. (The hard "candy" shell)
- The "soft chewy center" needs protecting, too.
- Firewalls can and are compromised.

Why Protect an Intranet?

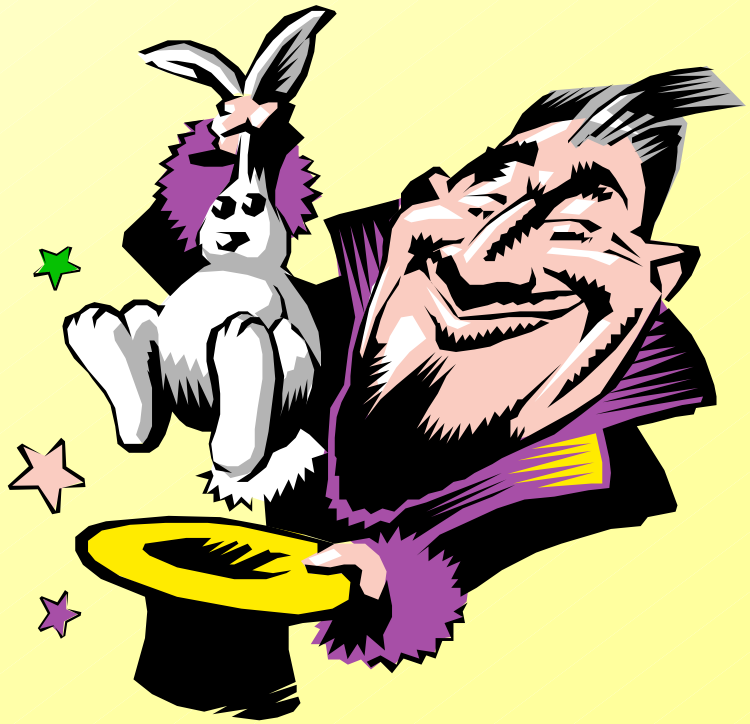
- As stated before, firewalls can and are compromised.
- The only secure system is a system with no input or output, but what good is it?
- Attacks also come from within the perimeter from vendors, contractors, and even employees.



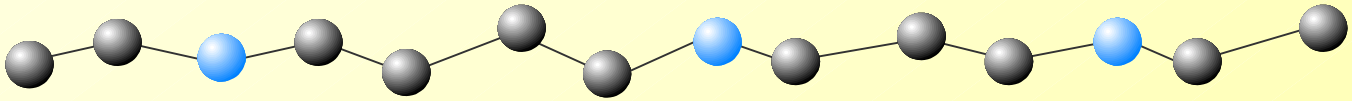
How Do I Begin?

It isn't magic; but don't start from scratch. Resources:

- Reference Books
- The Internet
- Consultation
- Off The Shelf Software

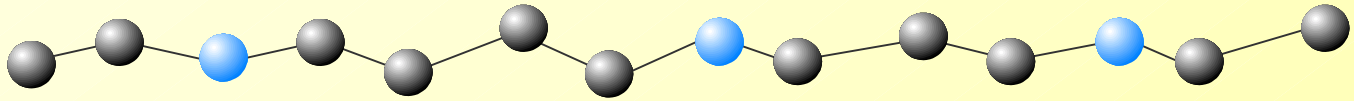


Awareness



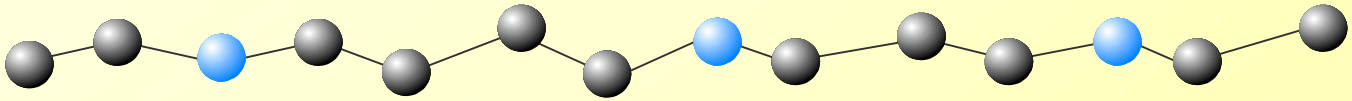
- Initial awareness program
  - Existing information dissemination methods
  - Special security awareness presentations
- Ongoing awareness (updates, etc.)
  - Security awareness newsletter
- New employee/contractor orientation

Implementation



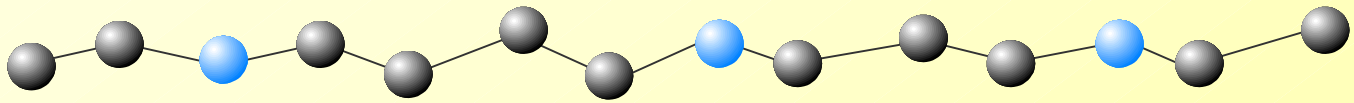
- Physical Constraints
  - Locks
    - Time Locks
    - Cipher Locks
  - “Man Traps”
  - “Tamper Proof” Containers

Implementation



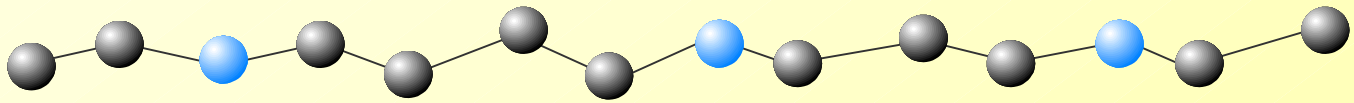
- Electronic Access
  - Proximity Badges
  - Biometrics (the Oldest Form of Authentication)
    - Fingerprint
    - Voice Recognition
    - Retinal Scan
    - Face Recognition
  - *Must* have human oversight!

Implementation



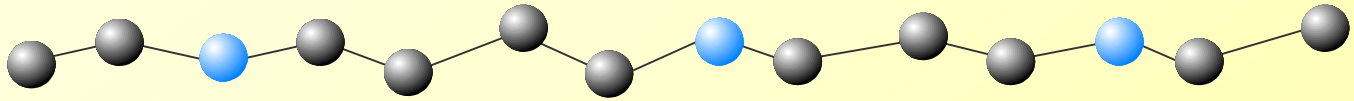
- Monitoring for Adherence to Established Practices and Policies.
  - Access logs (paper and electronic).
  - “Two man” accountability.
  - Visitor sign-in and escort.
  - Monitoring and review of video surveillance.
  - Regular audits (internal and external).
  - Mechanized scans of logs for anomalies.

Implementation



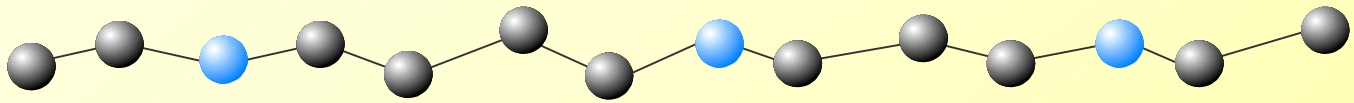
- Computer Access Controls.
  - Logon ID and Password
  - Digital Certificate/Smart Card
  - Hard Token (i.e. SecureID)
  - Biometrics
  - Integrated with Physical Access Method?
  - Logging! (with Review)
  - Regular Audits of Access Lists

Implementation



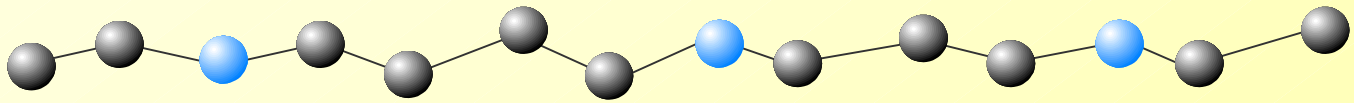
- Access Authorization
  - Role based
  - Specific Individual
  - Dependent on Authentication Mechanism
  - High Level
    - Corporate Directory
    - CORBASec ADO (Access Decision Object)
  - Granular
    - CORBA RAD (Resource Access Decision)

Policy Implementation



- Integration of Physical and Computer Security Policies and Procedures.
- Usability Studies.
- Log, Review, Audit.
- ***Consider*** Outside Certification.
- ***Nothing*** Can Replace the Human Mind and the Human Eye for Monitoring and Review.

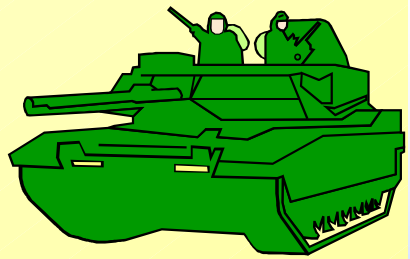
Logging



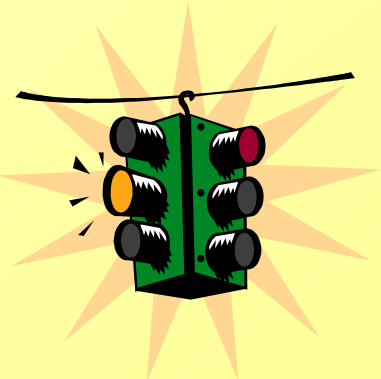
- Turn on logging!
- Allocate headcount to review logs.
- Train reviewer(s).
- Policy should dictate actions specifically.
  - Shut down intruder(s) immediately or
  - Track intruder to determine intent/build case.
  - Honeypot?

Enforcement

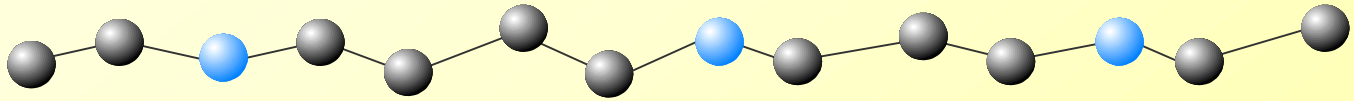
- Manual
  - Review system logs
  - Network/platform scans
  - Various periodic audits



- Automatic
  - Platform password restrictions
  - Firewalls, proxies, etc.
  - Various policy enforcement tools

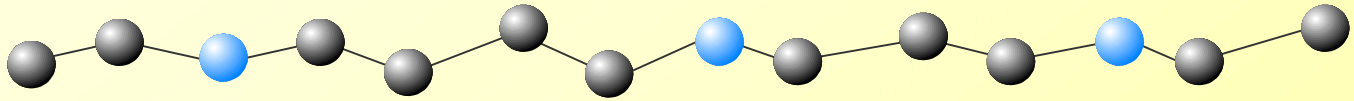


Policies



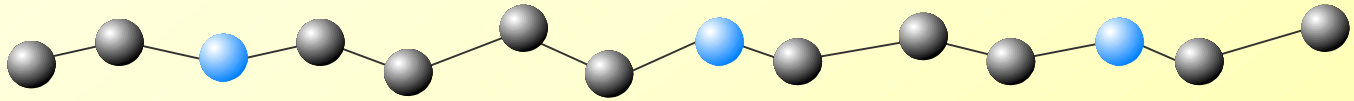
- ***Must*** Be Documented
- Clear, Concise, Well Indexed, Available
- Consider Online, Web Based
- Various Products Can “Jump Start” the Creation and Maintenance of Policies
- Regular Reviews
- ***Communication, Communication, Communication!***

Some Resources



- ICSA White Paper on Computer Crime **Statistics**
  - http://www.trusecure.com/html/tspub/whitepapers/crime.pdf
- http://www.securityfocus.com/vulns/stats.shtml
- … but don't always believe **Statistics**
  - http://www.attrition.org/errata/stats.html

More Resources



- Information Security Policies Made Easy – Version 7; by Charles Cresson Wood
- Secrets & Lies – Digital Security in a Networked World; by Bruce Schneier
- http://csrc.nist.gov
- http://www.security-policy.org
- http://www.msb.edu/faculty/culnanm/gippshome.html

Thanks for Listening

Sam Lumpkin

and

Marty Byrne

info@2ab.com

2AB, Inc.

205-621-7455

www.2ab.com