# CO 325: Computer and Network Security

## Introduction to Network Security

# Recognition

*This presentation contains slides that are copied and adapted from various sources, including the CCNA Security Certification Exam Lecture slides at www.cs.rpi.edu and Security Threat Reports from Symantec and Cisco*

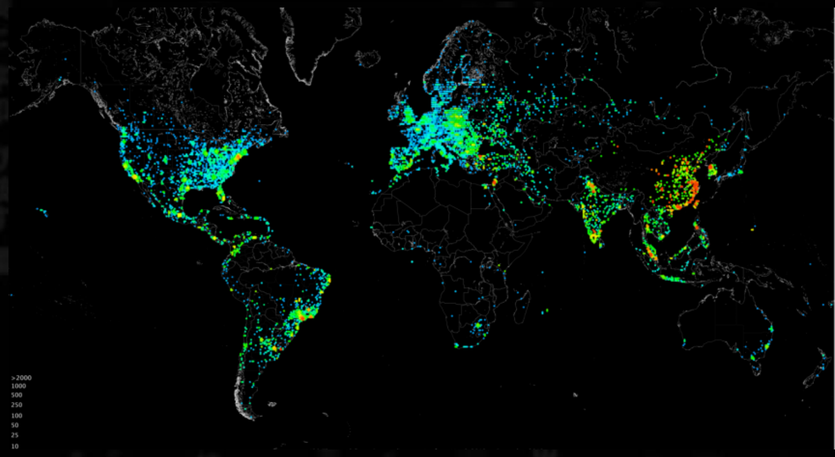
# What is Network Security?

Network security is the protection of
***information,***
and
***systems and hardware that use, store, and transmit that information.***

Network security encompasses those steps that are taken to ensure the ***confidentiality***, ***integrity***, and ***availability*** of data or resources.

# Rationale for Network Security

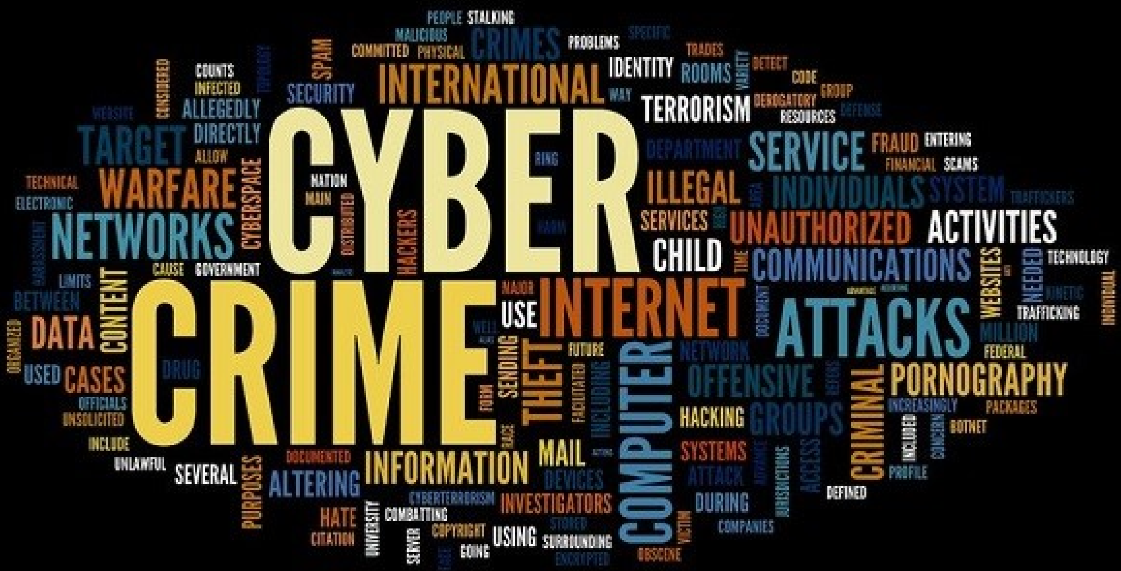
- The need for network security and its growth are driven by many factors:
  - Internet connectivity is 24/7 and is worldwide
  - Increase in cyber crime
  - Impact on business and individuals
  - Legislation & liabilities
  - Proliferation of threats
  - Sophistication of threats
  - Move towards Internet of Things



# Cyber Crime

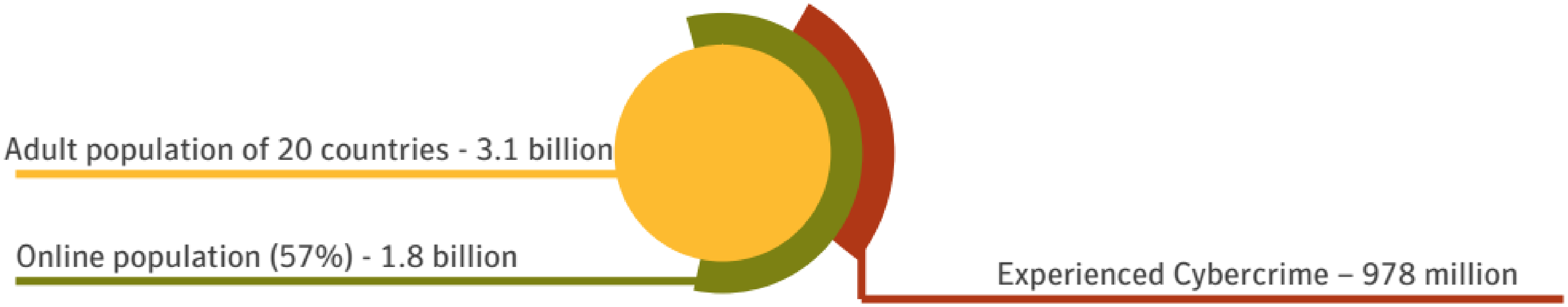
- Fraud/Scams
- Identity Theft
- Cyber Terrorism
- Cyber Extortion

- Harassment/Intimidation
- Obscene or Offensive content
  - E.g., Child Pornography



# Business Impact

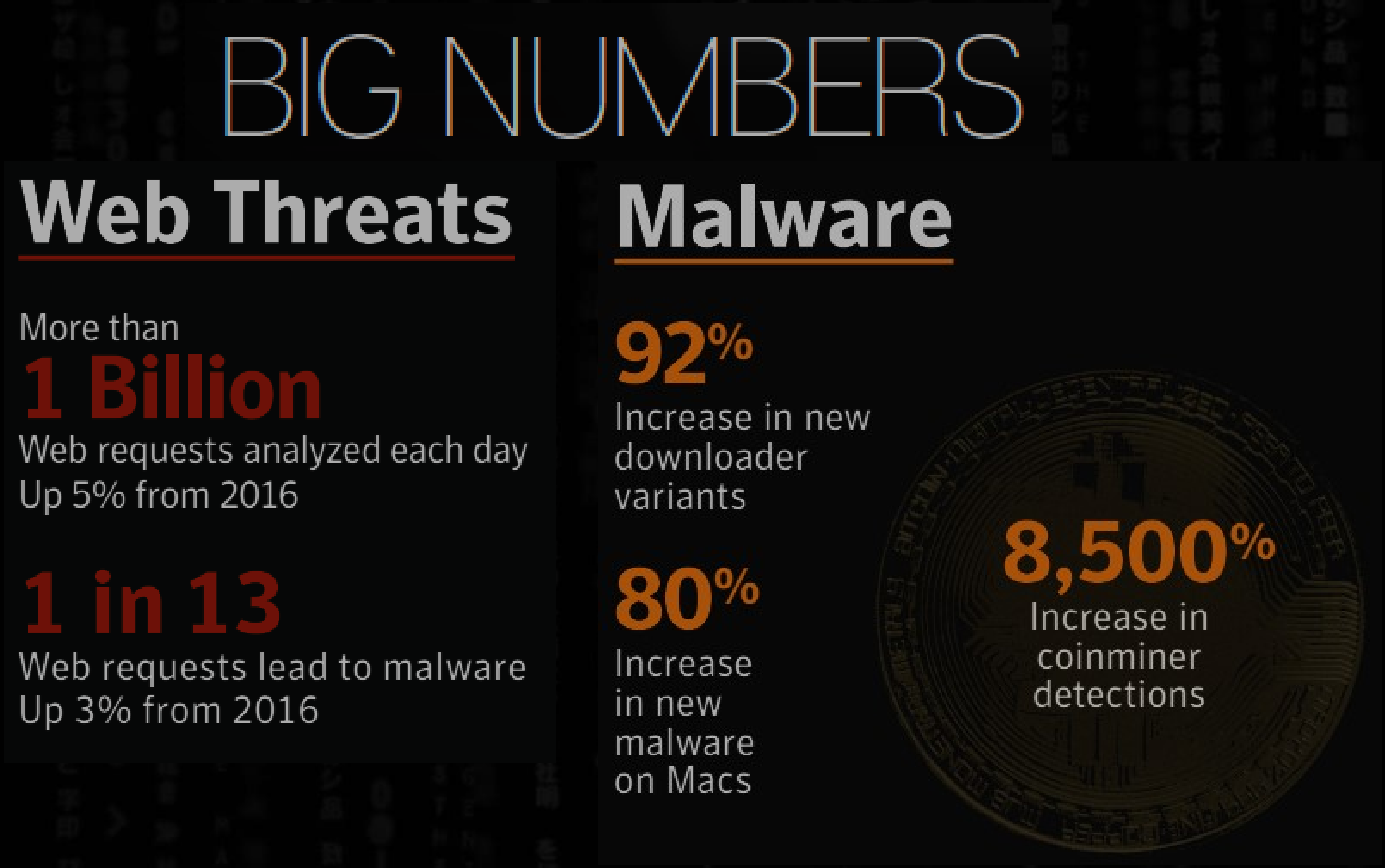
- Decrease in Productivity
- Loss of sales revenue
- Release of unauthorized sensitive data
- Threat of trade secrets or formulas
- Compromise of reputation and trust
- Loss of communications
- Threat to environmental and safety systems
- Loss of time



**Consumers who were victims of cybercrime globally lost $172 billion**

**The average victim lost $142**

# Proliferation of Threats



BIG NUMBERS

## Web Threats

More than
**1 Billion**
Web requests analyzed each day
Up 5% from 2016

**1 in 13**
Web requests lead to malware
Up 3% from 2016

## Malware

**92%**
Increase in new downloader variants

**80%**
Increase in new malware on Macs

**8,500%**
Increase in coinminer detections

# Proliferation of Threats

## BIG NUMBERS

### Email

Percentage spam rate

2015
53%

2016
53%

2017
55%

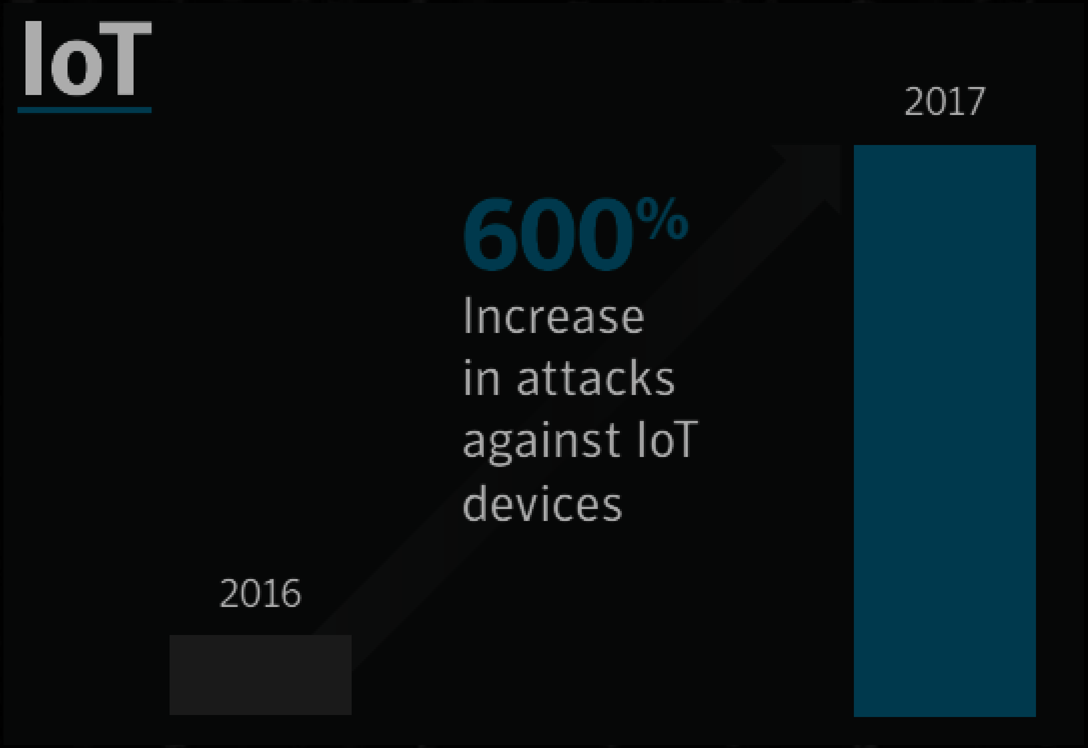
### Ransomware

5.4B
WannaCry attacks blocked

46%
Increase in new ransomware variants

# Proliferation of Threats

## BIG NUMBERS

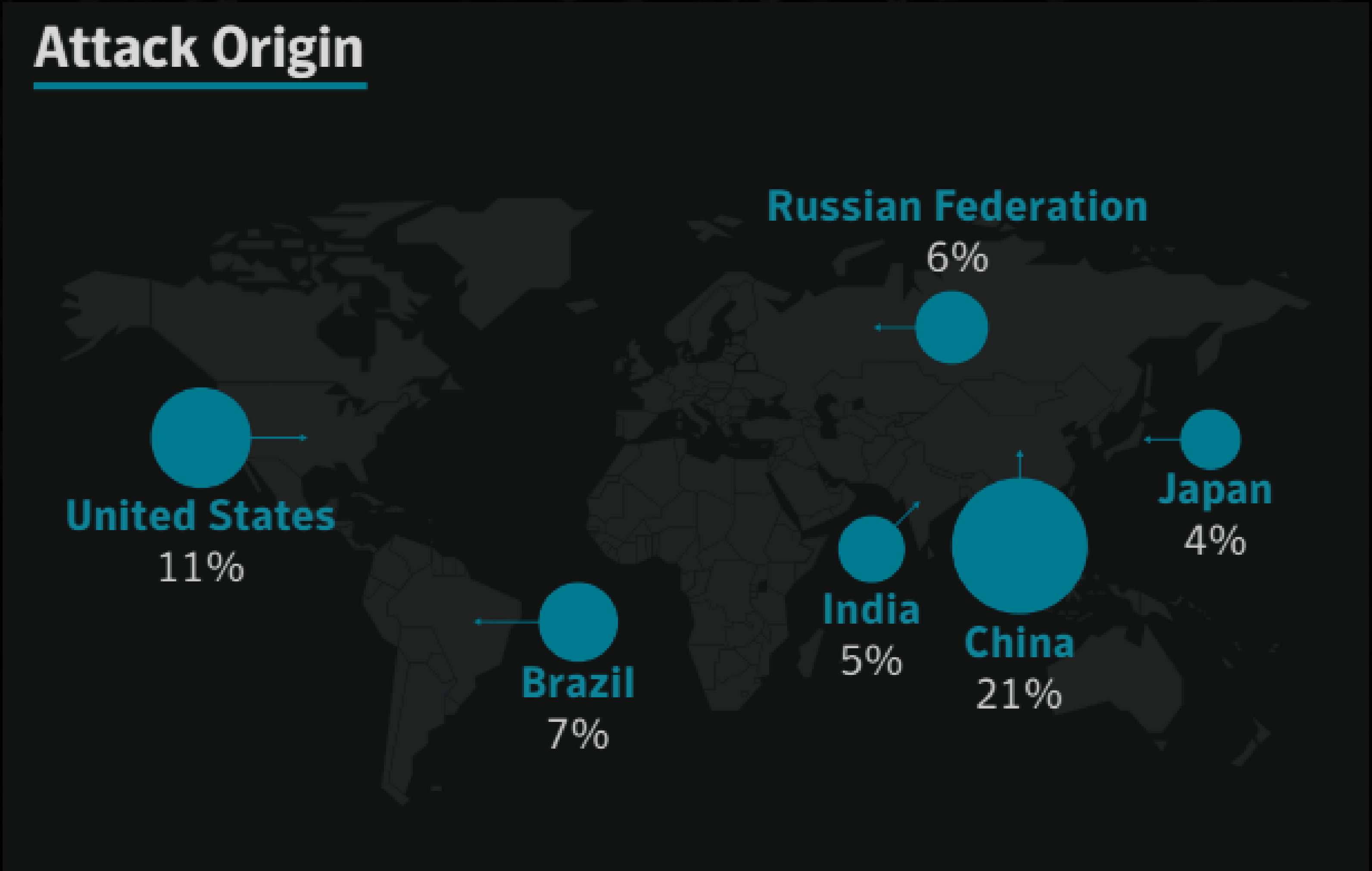


600%

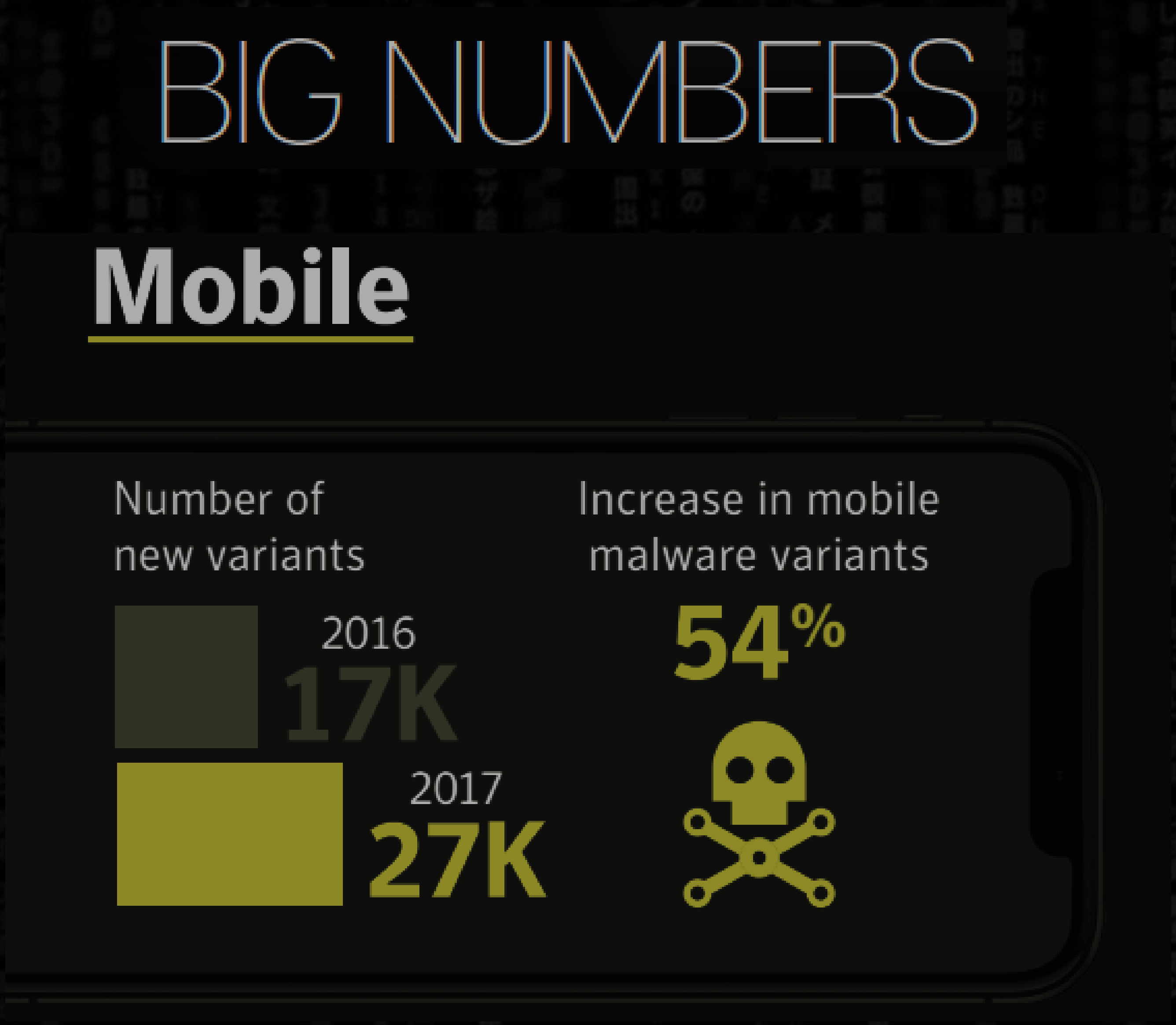
Increase in attacks against IoT devices

# Proliferation of Threats

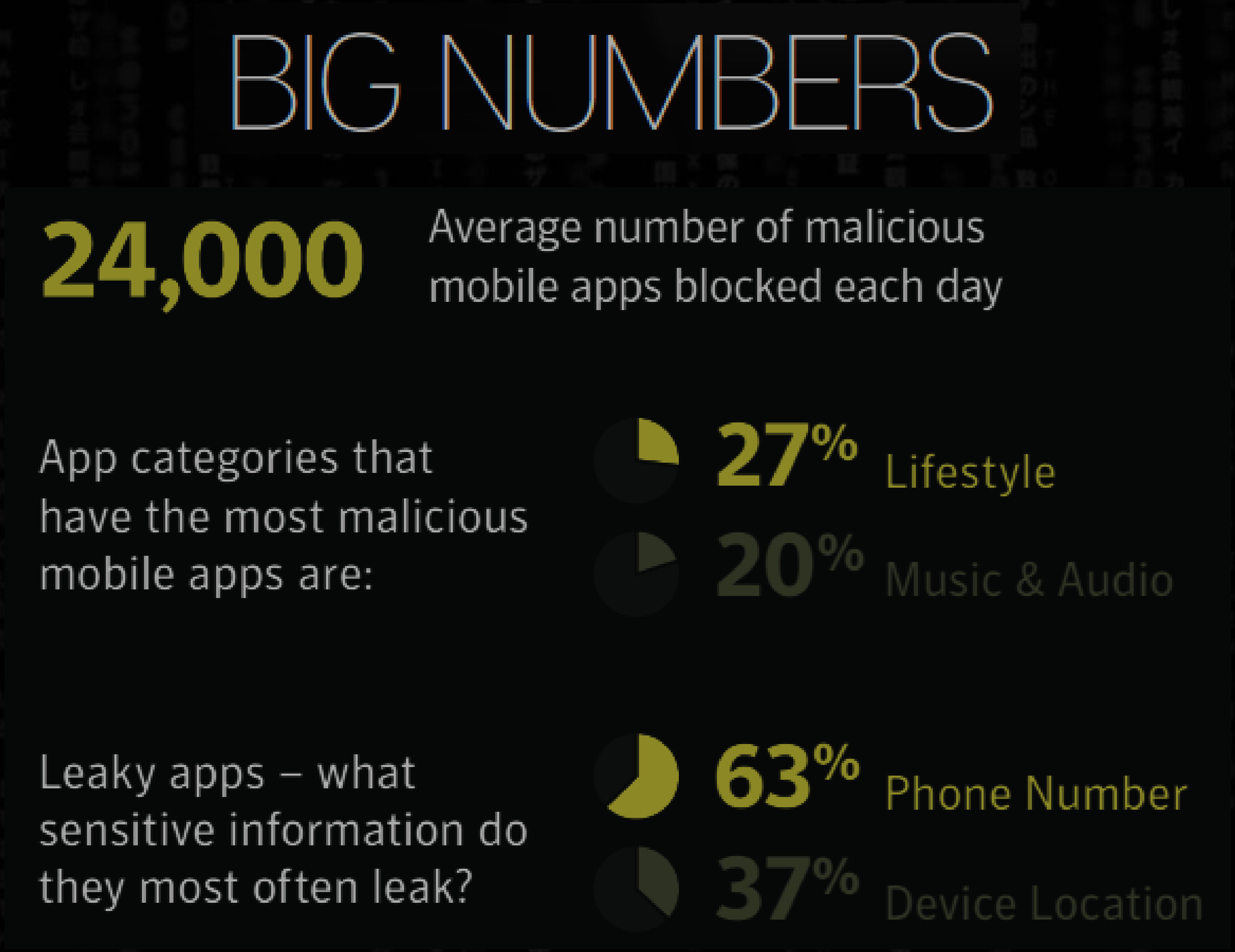
BIG NUMBERS



# Proliferation of Threats



# Proliferation of Threats



## BIG NUMBERS

**24,000** Average number of malicious mobile apps blocked each day

App categories that have the most malicious mobile apps are:

**27%** Lifestyle

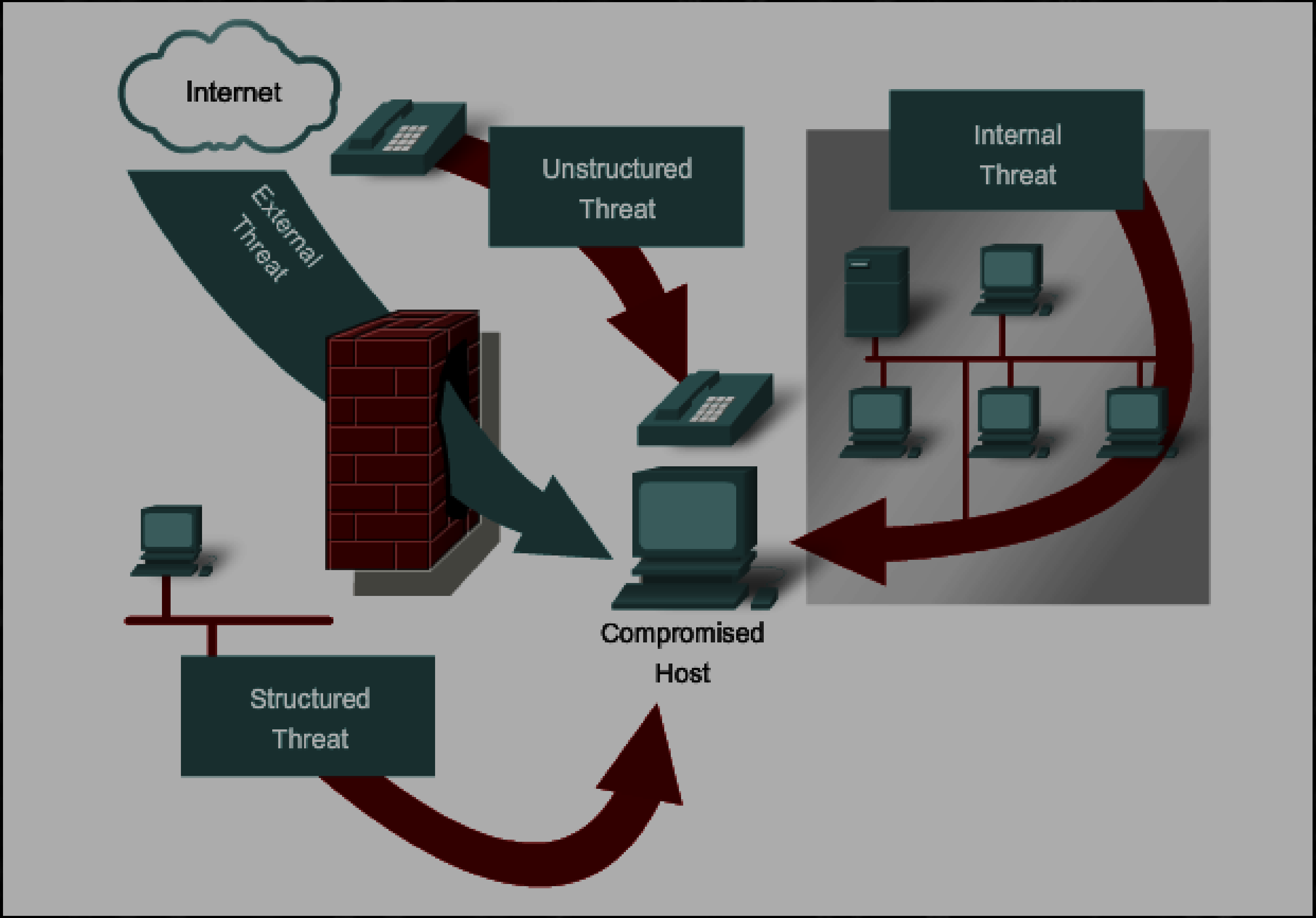
**20%** Music & Audio

Leaky apps – what sensitive information do they most often leak?

**63%** Phone Number

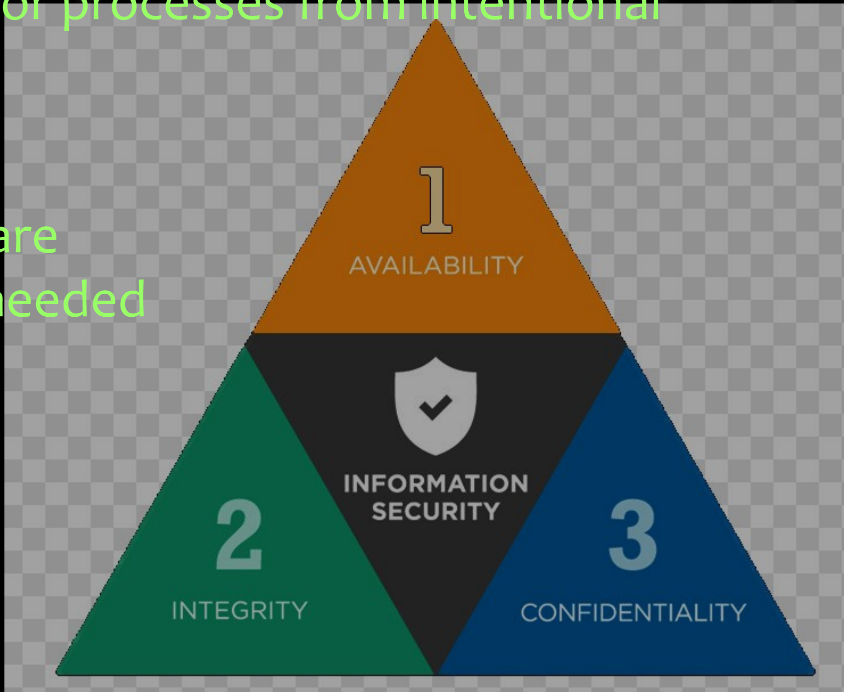
**37%** Device Location

# Sophistication of Threats

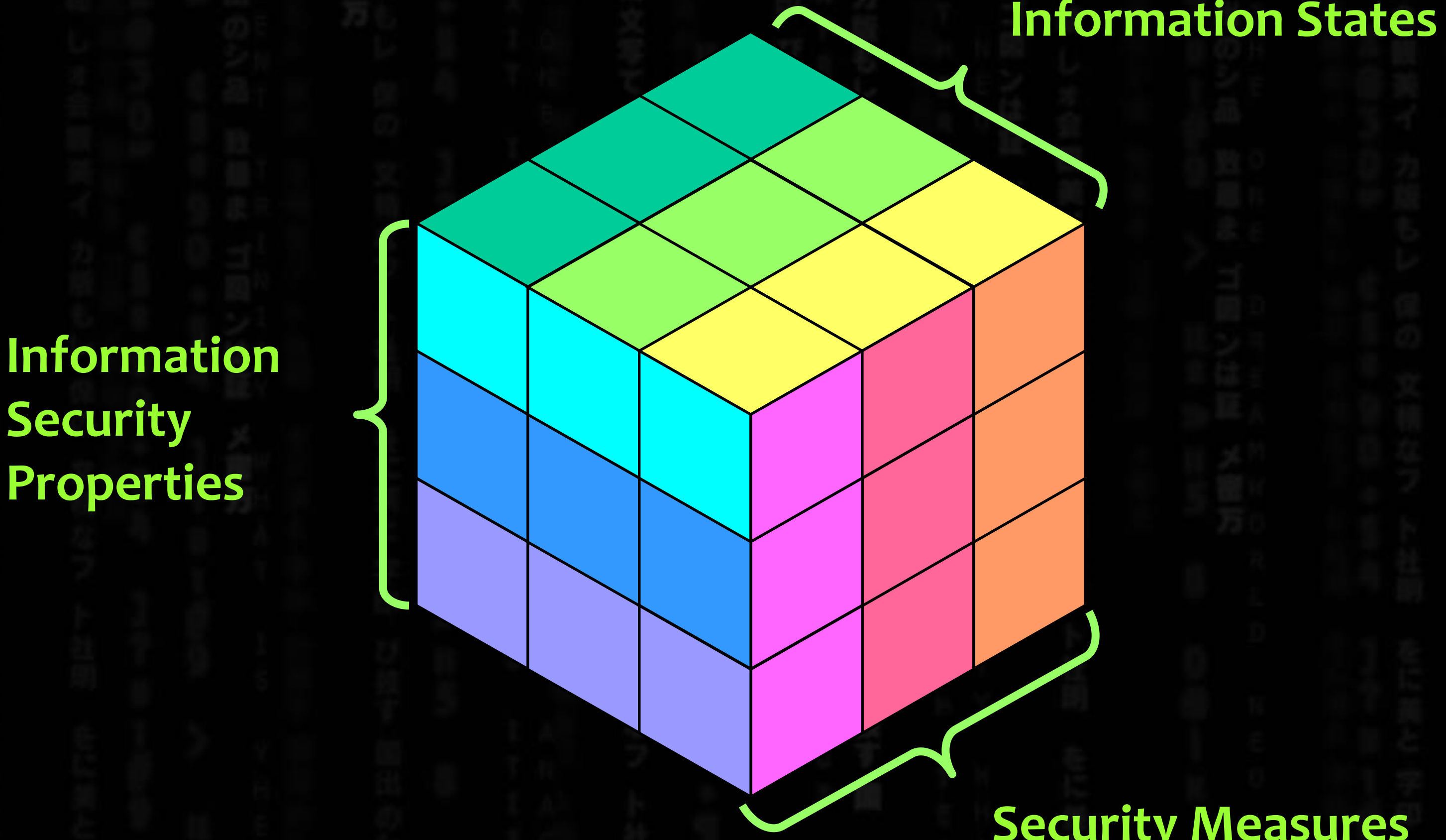


# Goals of an Information Security Program

- **Confidentiality**
  - ✓ Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- **Integrity**
  - ✓ The protection of system information or processes from intentional or accidental modification
- **Availability**
  - ✓ The assurance that systems and data are accessible by authorized users when needed

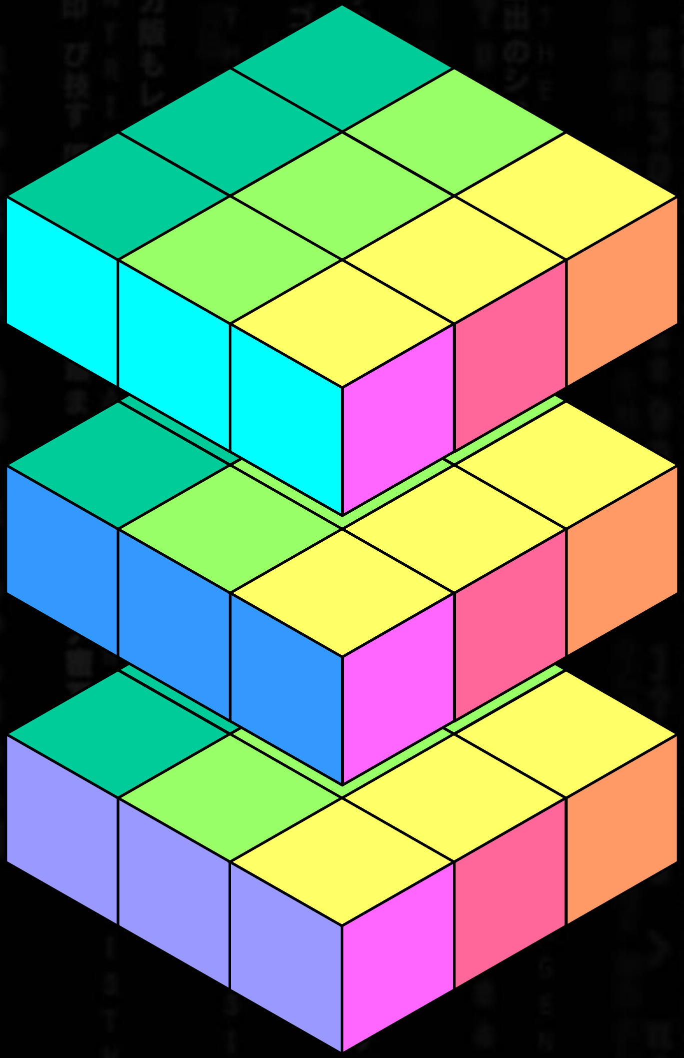


# Information Security Model



## McCumber Cube

# Information Security Properties

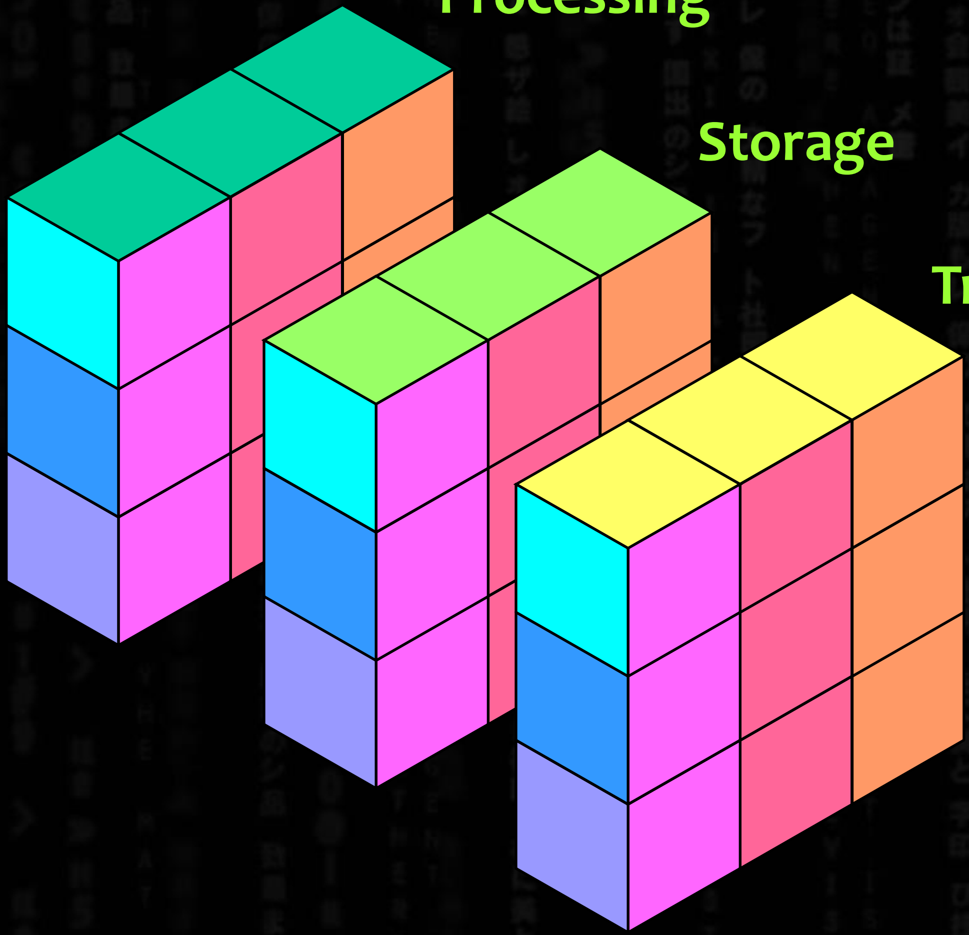


Confidentiality

Integrity

Availability

# Information States

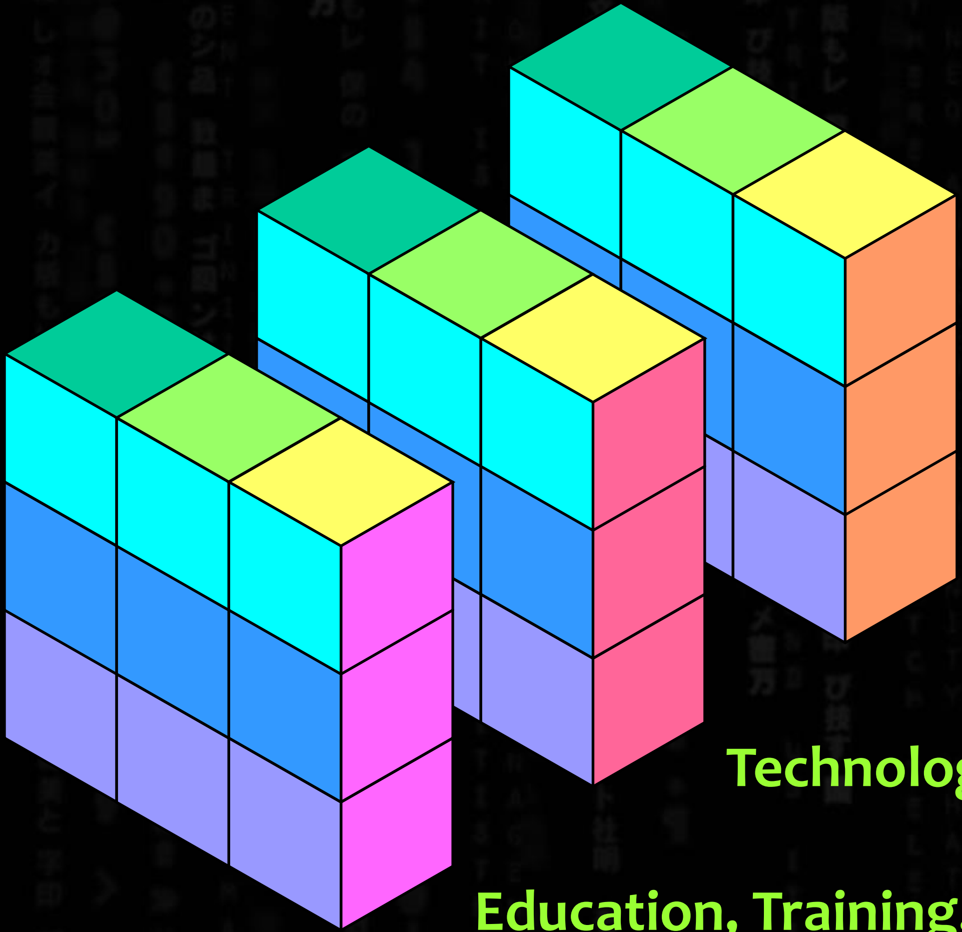


Processing

Storage

Transmission

# Security Measures

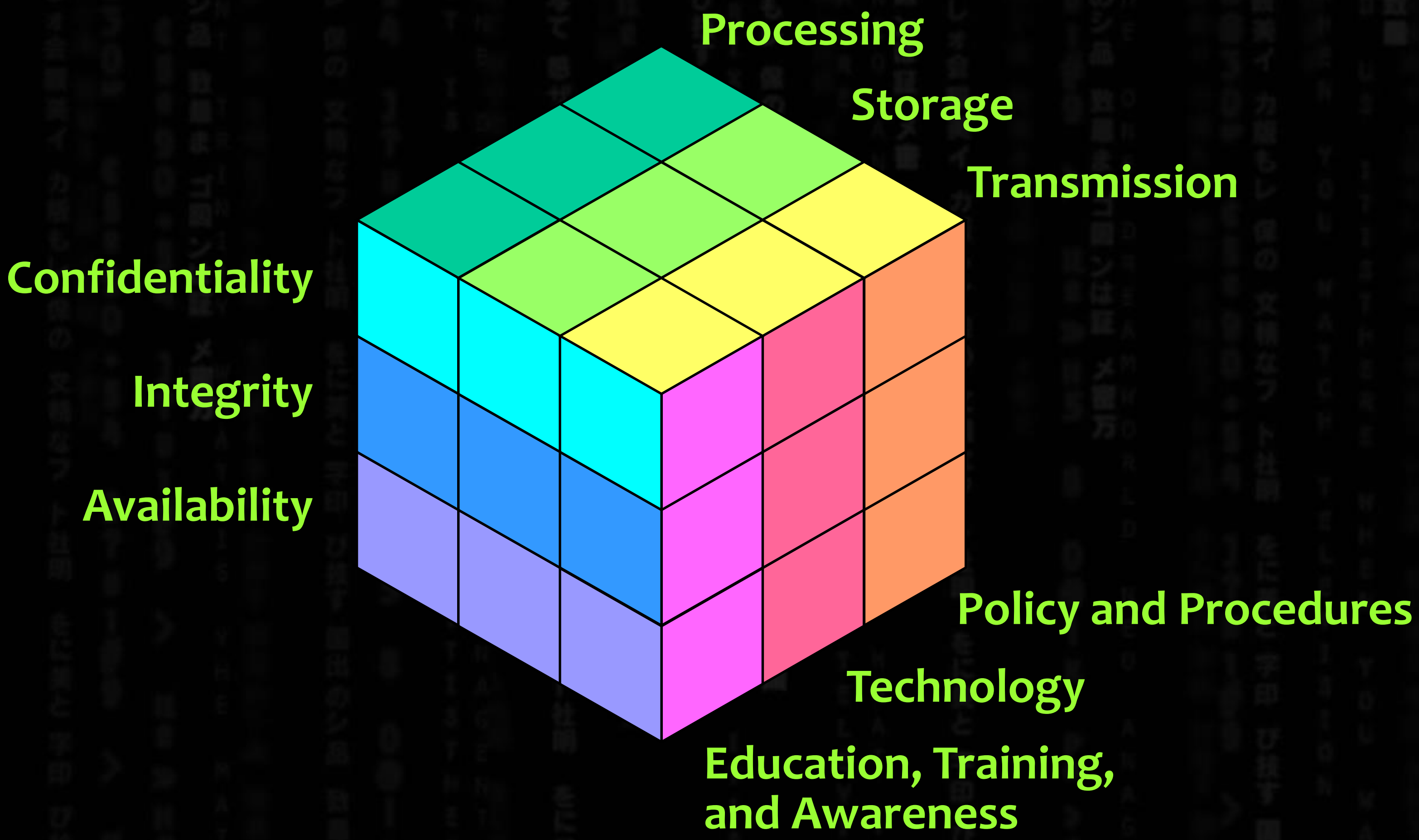


Policy and Procedures

Technology

Education, Training, and Awareness

# Information Security Model



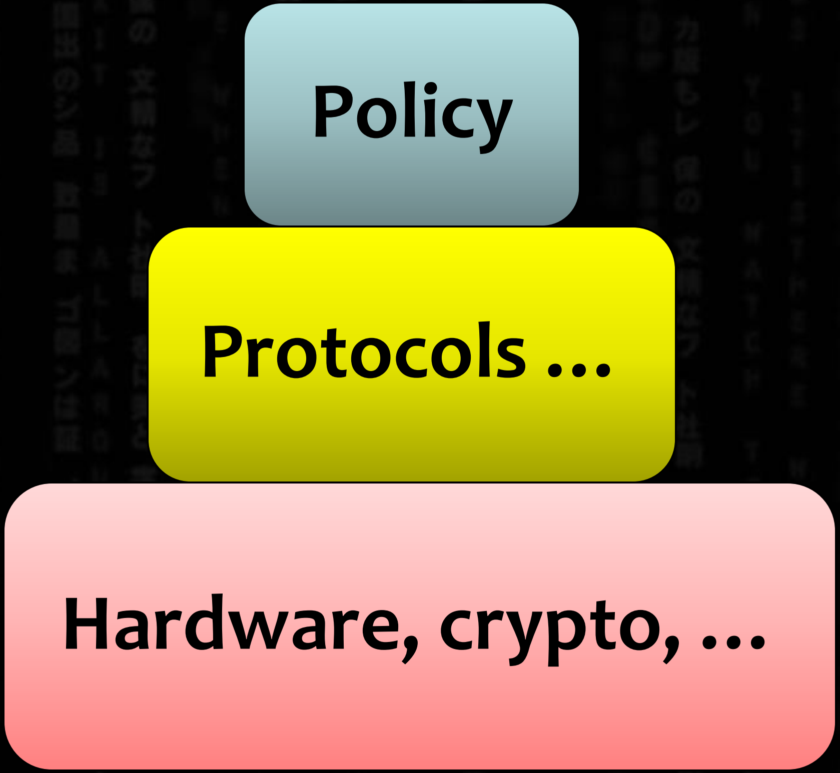
# Security Engineering

- Security engineering is about building systems to remain dependable in the face of malice, error and mischance.

- As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

# Security Engineering: Design Hierarchy

- What are we trying to do?
- How?
- With what?



Policy

Protocols ...

Hardware, crypto, ...

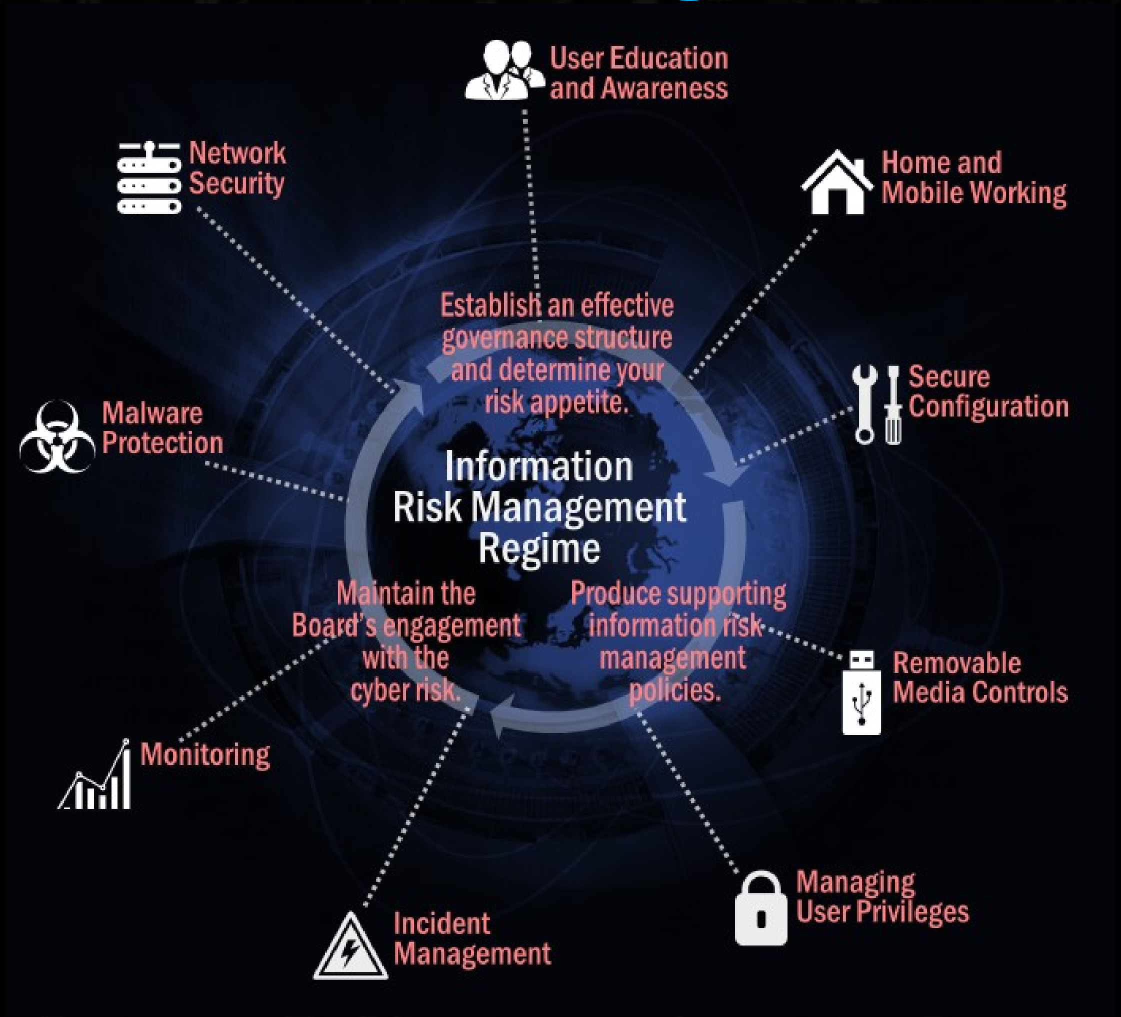
# Security vs. Dependability

- *Dependability = reliability + security*
- Reliability and security are often strongly correlated in practice
- But malice is different from error!
  - Reliability: “Bob will be able to read this file”
  - Security: “Enemy countries won’t be able to read this file”
- Proving a negative can be much harder …

# Risk Management

- Risk Analysis/Assessment
  - Assets
  - Threats
  - Vulnerabilities
  - Countermeasures
- Risk Mitigation
- Risk Communication
- Risk monitoring and review

# Risk Management

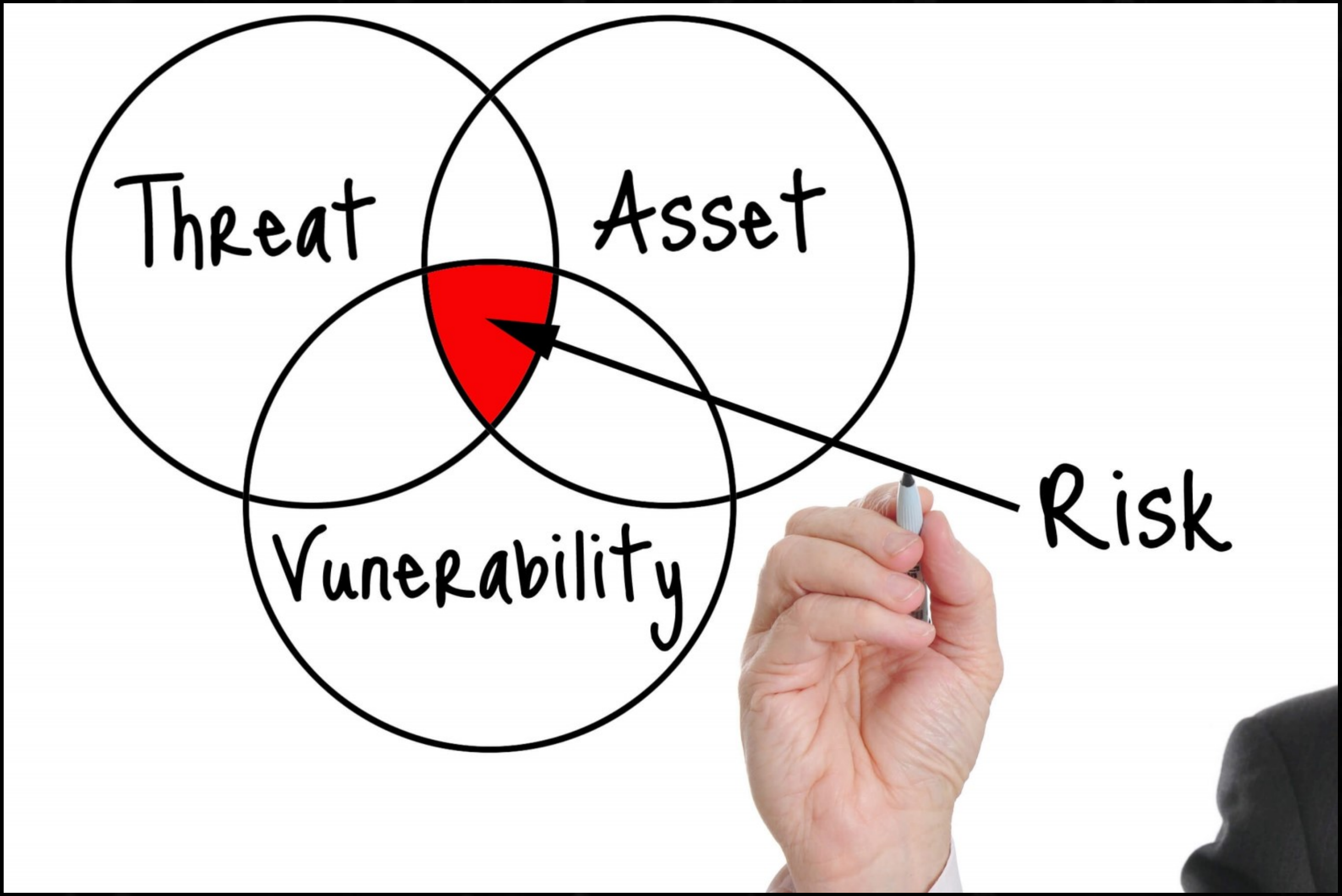

User Education and Awareness
Network Security
Home and Mobile Working
Establish an effective governance structure and determine your risk appetite.
Malware Protection
Secure Configuration
Information Risk Management Regime
Maintain the Board's engagement with the cyber risk.
Produce supporting information risk management policies.
Removable Media Controls
Monitoring
Managing User Privileges
Incident Management

- ➢ The process of assessing and quantifying risk and establishing an acceptable level of risk for the organization.
- ➢ Risk can be mitigated, but cannot be eliminated.

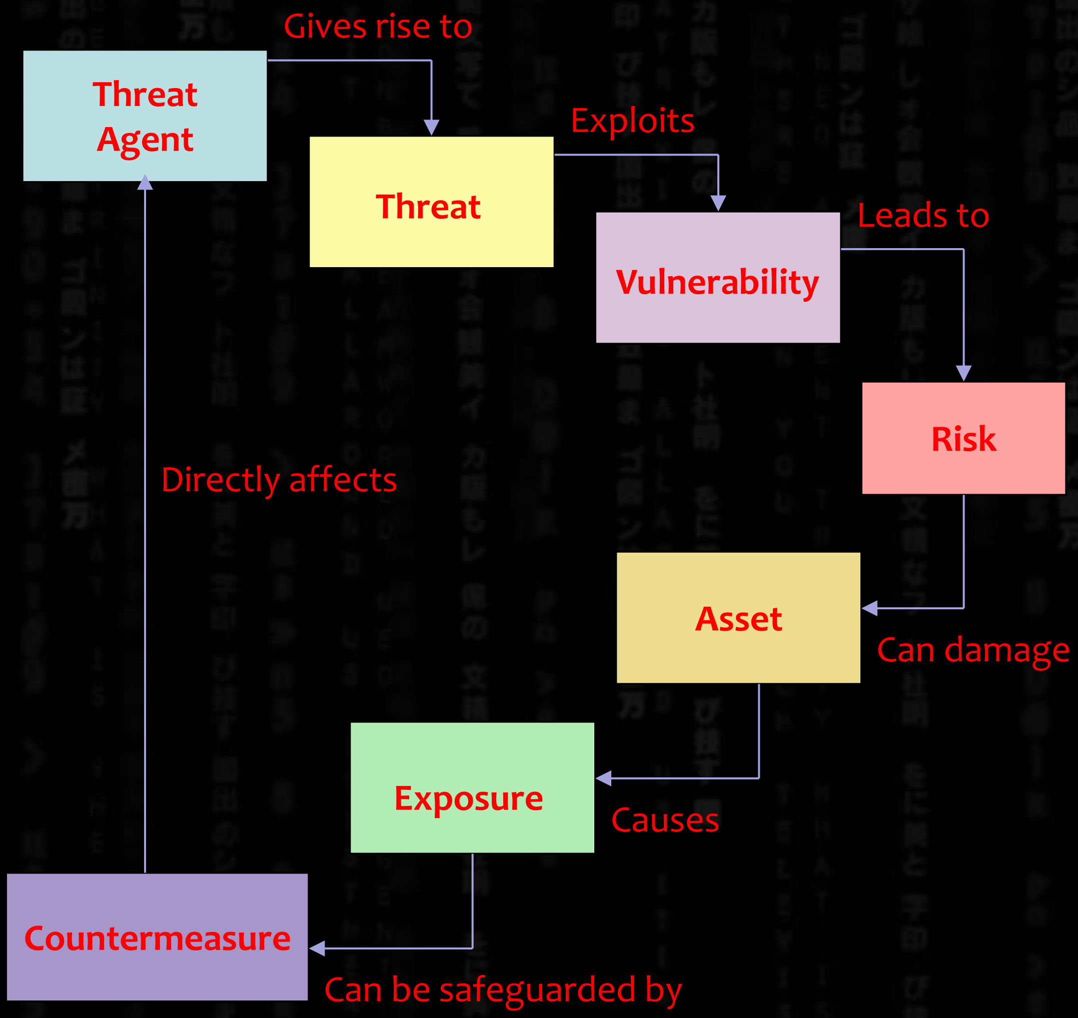
# Risk Management Terms

- **Vulnerability:** a system, network or device weakness
- **Threat:** potential danger posed by a vulnerability
- **Threat agent:** the entity that identifies a vulnerability and uses it to attack the victim
- **Risk:** likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- **Exposure:** potential to experience losses from a threat agent
- **Countermeasure:** put into place to mitigate the potential risk

# Risk Assessment



# Understanding Risk



Threat Agent

Gives rise to

Threat

Exploits

Vulnerability

Leads to

Risk

Asset

Can damage

Exposure

Causes

Countermeasure

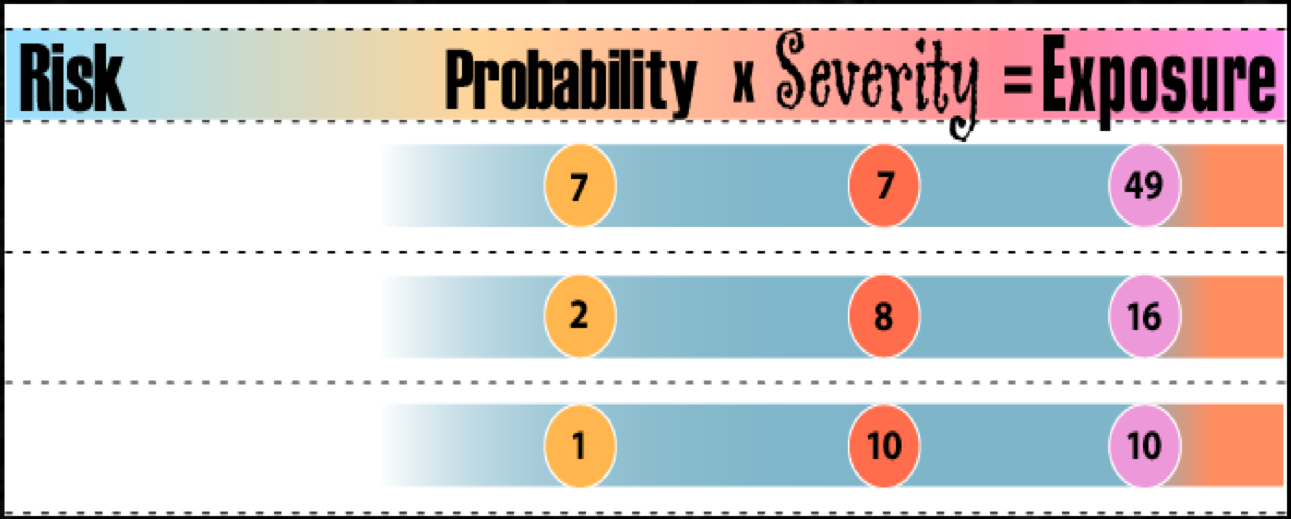
Can be safeguarded by

Directly affects

# Qualitative Risk Analysis

**Probability x Severity = Exposure**

**Exposure values prioritize the order for addressing risks**



| Risk | Probability | x Severity | = Exposure |
|---|---|---|---|
| A new worm | 7 | 7 | 49 |
| Web site defacement | 2 | 8 | 16 |
| Fire protection system Floods datacenter | 1 | 10 | 10 |

# Quantitative Risk Analysis

- Exposure Factor (EF)
  - % of loss of an asset
- Single Loss Expectancy (SLE)
  - EF x Value of asset
- Annualized Rate of Occurrence (ARO)
  - A number representing frequency of occurrence of a threat

    Example: 0.0 = Never 1000 = Occurs very often
- Annualized Loss Expectancy (ALE)
  - Monetary value derived from: SLE x ARO

# Asset Identification

- Categories of assets
  - Information Assets (people, hardware, software, systems)
  - Supporting Assets (facilities, utilities, services)
  - Critical Assets (can be either of those listed above)
- Attributes of the assets need to be compiled
- Determine each item’s relative value
  - How much revenue/profit does it generate?
  - What is the perceived loss (tangible & intangible)
  - What is the cost to replace it?
  - How difficult would it be to replace?
  - How quickly can it be replaced?

# Network Security "Threat"

- A potential danger to information or a system
  - E.g., the ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network
- There may be weaknesses that greatly increase the likelihood of a threat manifesting
- Threats may include equipment failure structured attacks, natural disasters, physical attacks, theft, viruses and many other potential events causing danger or damage

# Types of Network Threats

- Viruses, worms and Trojan horses
- Spyware, adware and ransomware
- Phishing and spam
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

# Vulnerability

- A network vulnerability is a weakness in a system, technology, product or policy
- In today's environment, several organizations track, organize and test these vulnerabilities
- Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- The common vulnerability exposure (CVE) list also publishes ways to prevent the vulnerability from being attacked

# Vulnerability Appraisal

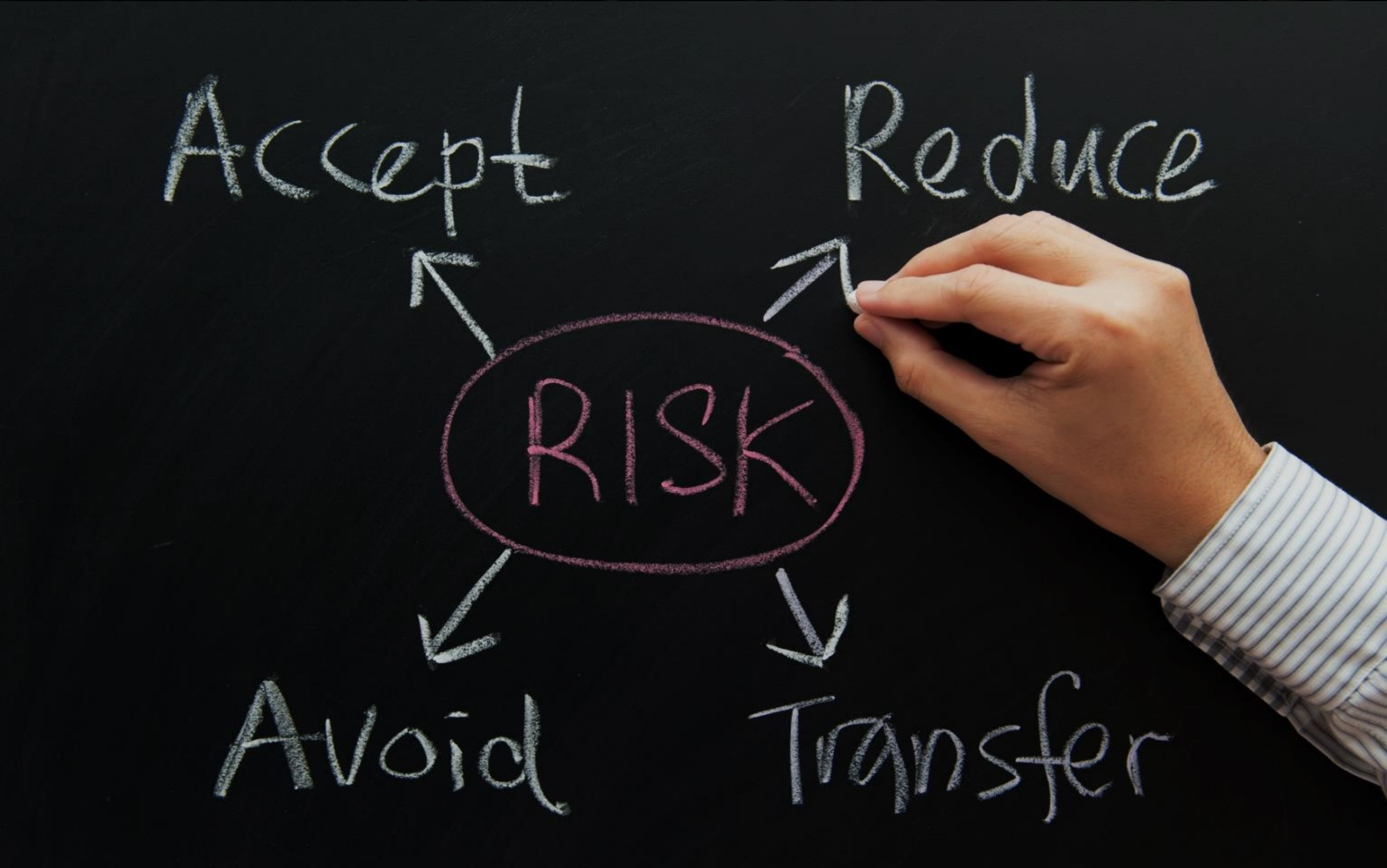
- Vulnerability appraisal is a critical, yet often neglected, part of network security risk management
- A vulnerability appraisal is a snapshot of the security of the organization as it now stands
  - i.e., What current security weaknesses may expose the assets to these threats?
- Vulnerability scanners are tools available as free Internet downloads and as commercial products
  - E.g., Nessus, OpenVAS, SAINT
- These tools compare the asset against a database of known vulnerabilities and produce a discovery report that exposes the vulnerability and assesses its severity

Nessus vulnerability scanner

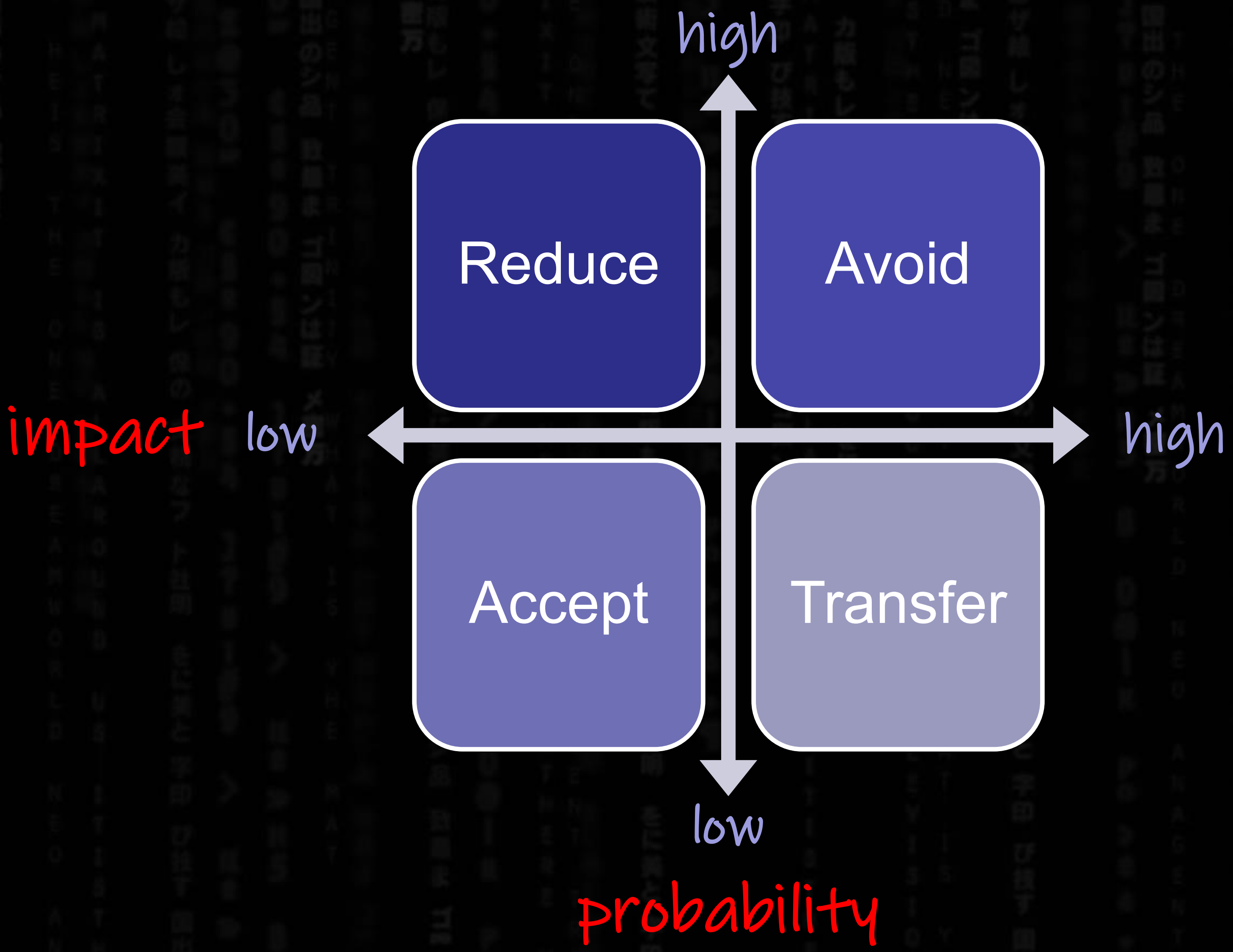
OpenVAS Open Vulnerability Assessment System

SAINT®

# Managing Risks



# Managing Risks



high

Reduce

Avoid

impact low

high

Accept

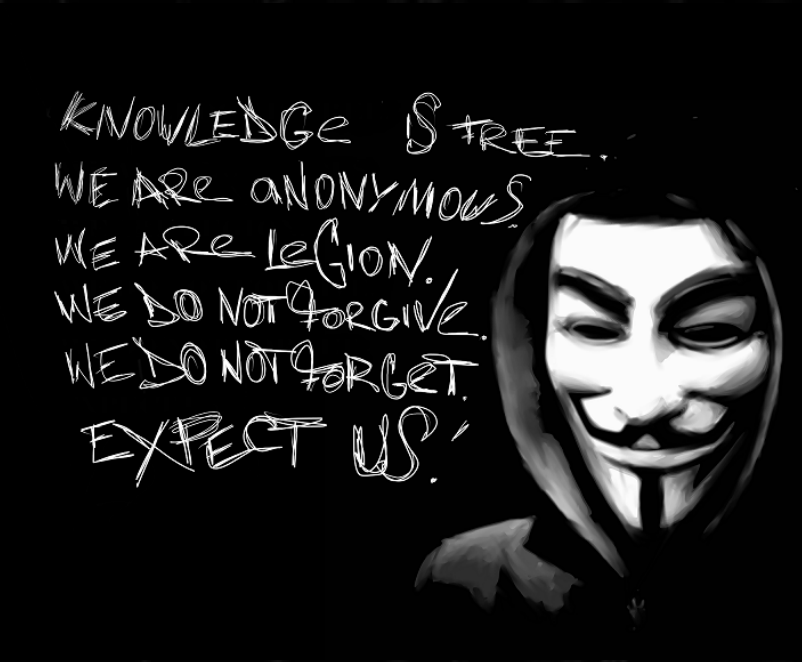
Transfer

low

probability

# Types of Attacks

- ***Structured attack***
  - Come from hackers who are highly motivated and technically competent.
  - They know the system vulnerabilities and can understand and develop exploit code and scripts.



# Types of Attacks

- ***Unstructured attack***
  - Consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.
  - Even unstructured threats that are only executed with the intent of testing and challenging a hacker’s skills can still do serious damage to a company.

MISSILE WARNING
SUB-LAUNCH DETECTION
Is it a game, or is it real?
WARGAMES
A Leonard Goldberg Production A John Badham Film "WARGAMES" MATTHEW BRODERICK DABNEY COLEMAN JOHN WOOD ALLY SHEEDY
Written by LAWRENCE LASKER & WALTER F. PARKES Director of Photography WILLIAM A. FRAKER, A.S.C. Music by ARTHUR B. RUBINSTEIN Executive Producer LEONARD GOLDBERG Produced by HAROLD SCHNEIDER
PG PARENTAL GUIDANCE SUGGESTED
SOME MATERIAL MAY NOT BE SUITABLE FOR CHILDREN
Directed by JOHN BADHAM
Produced in association with Sherwood Productions Panavision Metrocolor Read the Dell Book
DOLBY STEREO
DISTRIBUTED BY MGM/UA

# Types of Attacks

- ***External attacks***
  - Initiated by individuals or groups working outside of a company.
  - They do not have authorized access to the computer systems or network.
  - They gather information in order to work their way into a network mainly from the Internet or dialup access servers.
- ***Internal attacks***
  - More common and dangerous.
  - Internal attacks are initiated by someone who has authorized access to the network.
  - According to the FBI, internal access and misuse account for 60 to 80 percent of reported incidents.
  - These attacks often are traced to disgruntled employees.

# Top 10 Internal Network Vulnerabilities

- USB drives
- laptops and netbooks
- wireless access points
- miscellaneous USB devices (digital cameras, MP3 players, etc.)
- employees borrowing others’ machines or devices
- the Trojan Human (attackers who visit sites disguised as employee personnel or contractors)
- optical media (CDs, DVDs, etc.)
- lack of employee alertness
- smartphones
- e-mail

# Types of Attacks

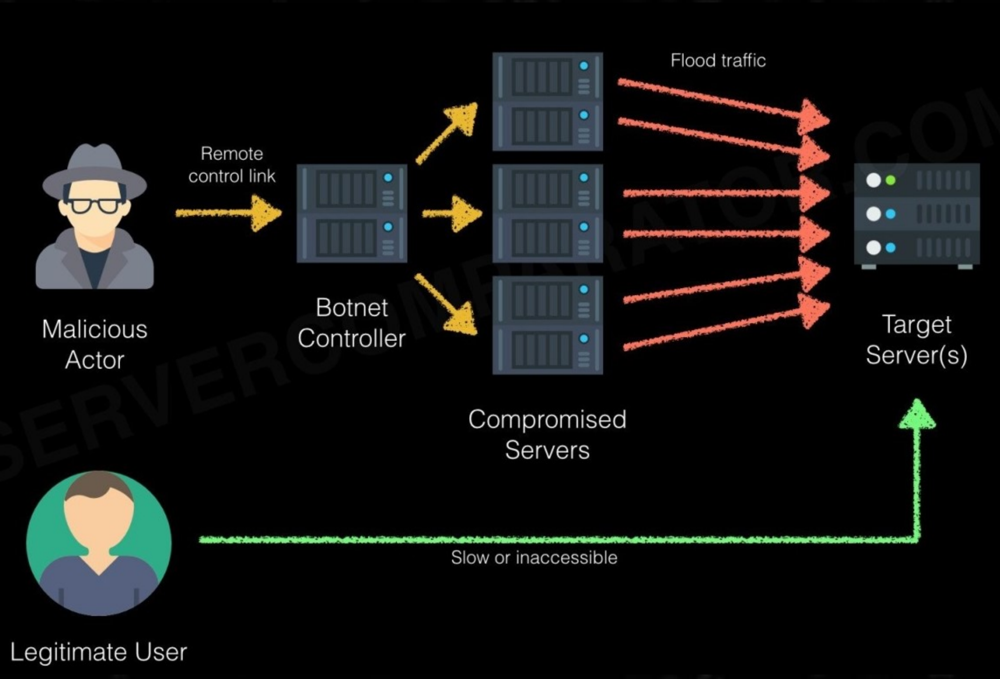
- Passive Attack
  - Listen to system passwords
  - Release of message content
  - Traffic analysis
  - Data capturing

- Active Attack
  - Attempt to log into someone else’s account
  - Wire taps
  - Denial of services
  - Masquerading
  - Message modifications

USERNAME
PASSWORD
Bad guys can secretly monitor what sites you visit
USERNAME
PASSWORD
Bad guys can steal your private information without you knowing

# Denial-of-Service (DoS) Facts

- Commonly used against information stores like web sites, DNS servers, etc.
- Simple and usually quite effective
- Does not pose a direct threat to sensitive data
- The attacker tries to prevent a service from being used and making that service unavailable to legitimate users
- Attackers typically go for high visibility targets such as the web server, or for infrastructure targets like routers and network links



# Denial-of-Service Example

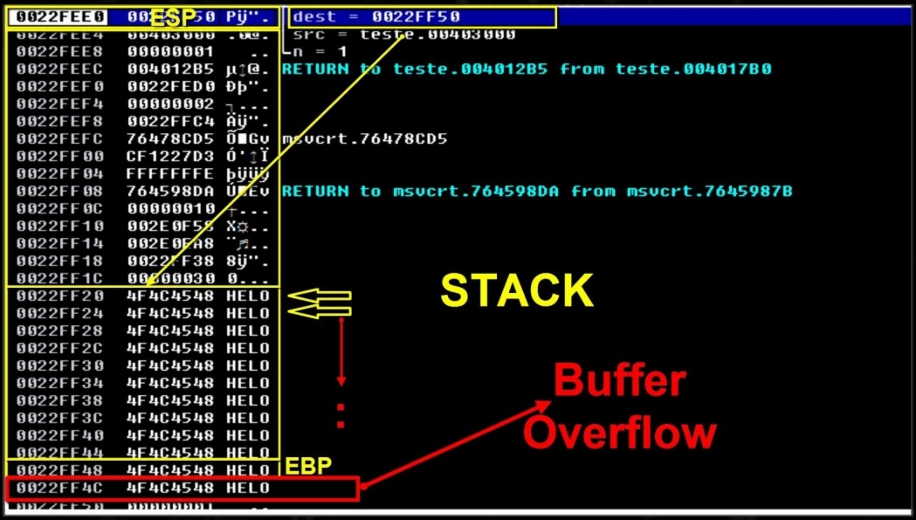
- If a mail server is capable of receiving and delivering 10 messages a second,
  - an attacker simply sends 20 messages per second.
  - The legitimate traffic (as well as a lot of the malicious traffic) will get dropped, or the mail server might stop responding entirely.
- This type of an attack may be used as a diversion while another attack is made to actually compromise systems
- In addition, administrators are likely to make mistakes during an attack and possibly change a setting that creates a vulnerability that can be further exploited

# Types of Denial-of-Service Attacks

- Buffer Overflow Attacks
- SYN Flood Attack
- Teardrop Attacks
- Smurf Attack
- DNS Attacks
- Email Attacks
- Physical Infrastructure Attacks
- Viruses/Worms

# DoS: Buffer Overflow Attacks

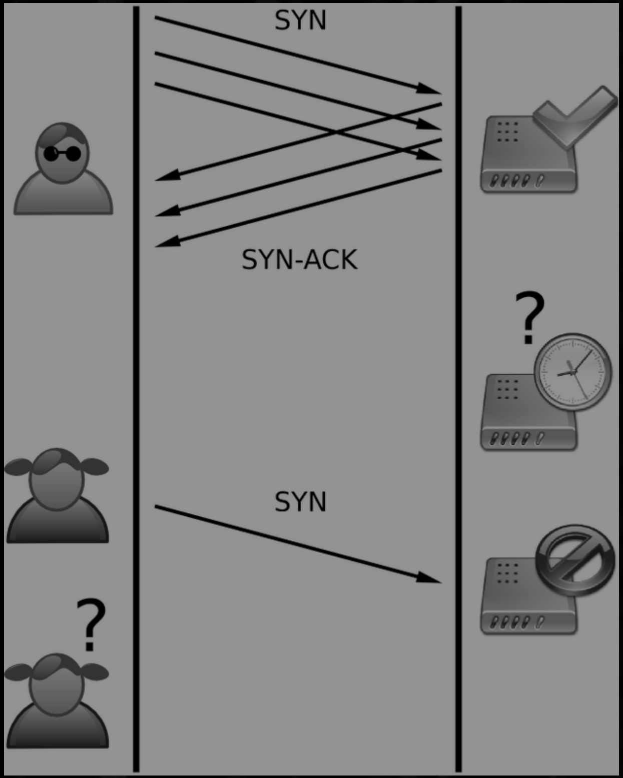
- The most common DoS attack exploits Buffer Overflow vulnerabilities in programs/processes.
  - Buffer overflow vulnerabilities are characterized by the overwriting of memory fragments of the process, which should have never been modified intentionally or unintentionally.
  - Overwriting values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, segmentation faults, and other errors to occur.

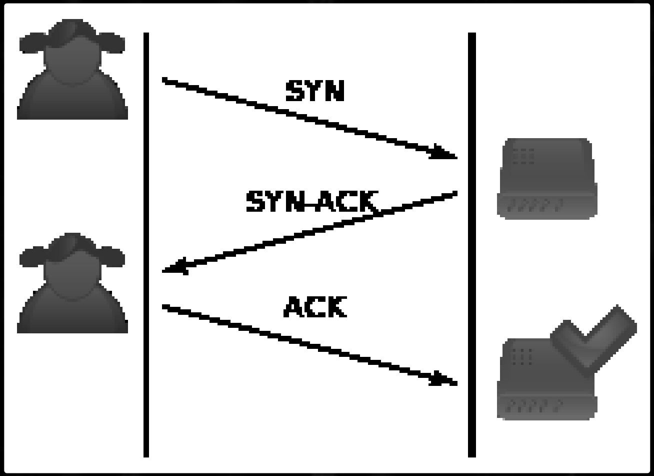


```
0022FEE0   0022FF50 Pÿ".   dest = 0022FF50
0022FEE4   00403000 .0@.   src = teste.00403000
0022FEE8   00000001    ..  n = 1
0022FEEC   004012B5 µ↕@.  RETURN to teste.004012B5 from teste.004017B0
0022FEF0   0022FED0 Ðþ".
0022FEF4   00000002 ┐...
0022FEF8   0022FFC4 Äÿ".
0022FEFC   76478CD5 Õ■Gv  msvcrt.76478CD5
0022FF00   CF1227D3 Ó'↕Ï
0022FF04   FFFFFFFE þÿÿÿ
0022FF08   764598DA Ú■Ev  RETURN to msvcrt.764598DA from msvcrt.7645987B
0022FF0C   00000010 ┼...
0022FF10   002E0F58 X☼..
0022FF14   002E0EA8 ¨♫..
0022FF18   0022FF38 8ÿ".
0022FF1C   00000030 0...
0022FF20   4F4C4548 HELO
0022FF24   4F4C4548 HELO
0022FF28   4F4C4548 HELO
0022FF2C   4F4C4548 HELO
0022FF30   4F4C4548 HELO
0022FF34   4F4C4548 HELO
0022FF38   4F4C4548 HELO
0022FF3C   4F4C4548 HELO
0022FF40   4F4C4548 HELO
0022FF44   4F4C4548 HELO
0022FF48   4F4C4548 HELO
0022FF4C   4F4C4548 HELO
0022FF50   00000001
```

# DoS: SYN Flood Attack

- When TCP connection sessions are initiated between a client and server in a network, the session-establishing packets include a SYN field that identifies the sequence order.
- A SYN flood is a DoS attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.



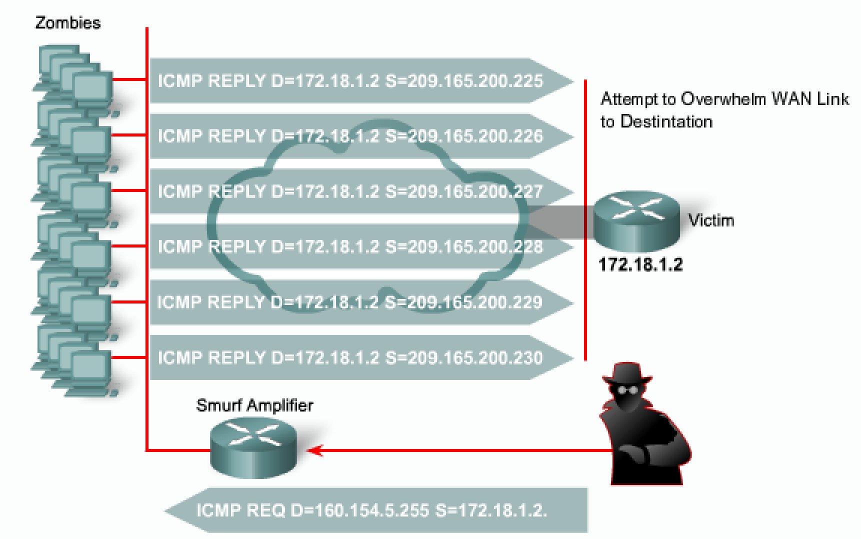


# DoS: Teardrop Attack

- Exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments.
- The fragmented packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system.
- In the teardrop attack, an attacker's IP puts a confusing value in the second or later fragment. If the receiving operating system cannot cope with such fragmentation, then it can cause the system to crash.

# DoS: Smurf Attack

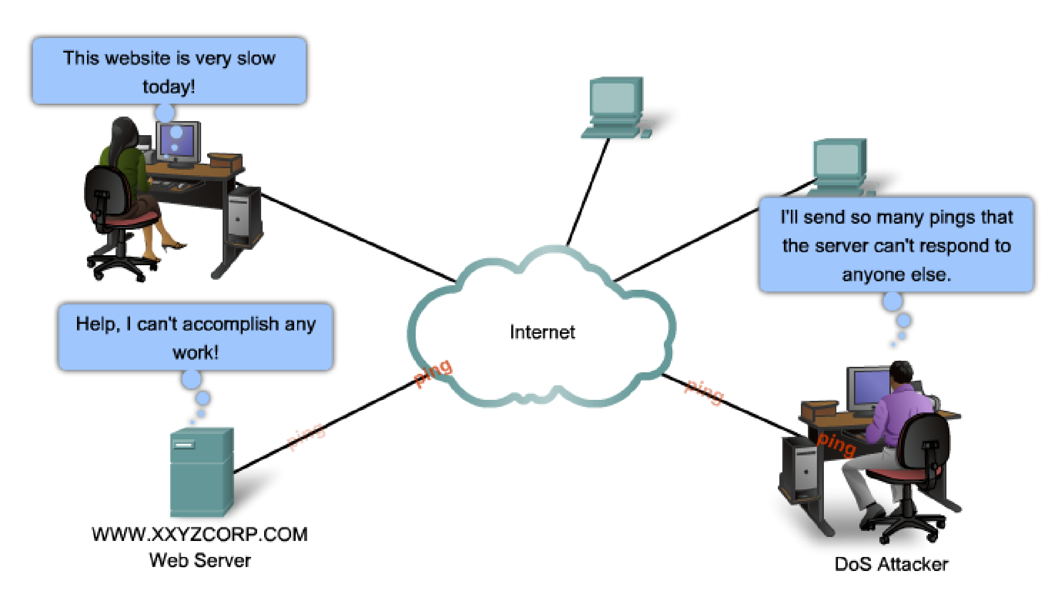
- The attacker sends an IP ping request to a network site.
- The ping packet requests that it be broadcast to a number of hosts within that local network.
- The packet also indicates that the request is from a different site, i.e. the victim site that is to receive the denial of service.


Zombies
ICMP REPLY D=172.18.1.2 S=209.165.200.225
ICMP REPLY D=172.18.1.2 S=209.165.200.226
ICMP REPLY D=172.18.1.2 S=209.165.200.227
ICMP REPLY D=172.18.1.2 S=209.165.200.228
ICMP REPLY D=172.18.1.2 S=209.165.200.229
ICMP REPLY D=172.18.1.2 S=209.165.200.230
Attempt to Overwhelm WAN Link to Destintation
Victim
172.18.1.2
Smurf Amplifier
ICMP REQ D=160.154.5.255 S=172.18.1.2.

- This is called IP Spoofing--the victim site becomes the address of the originating packet.
- The result is that lots of ping replies flood back to the victim host. If the flood is big enough then the victim host will no longer be able to receive or process "real" traffic.

# DoS: DNS Attacks

- A famous DNS attack was a DDoS "ping" attack. The attackers broke into machines on the Internet (popularly called "zombies") and sent streams of forged packets at the 13 DNS root servers via intermediary legitimate machines.

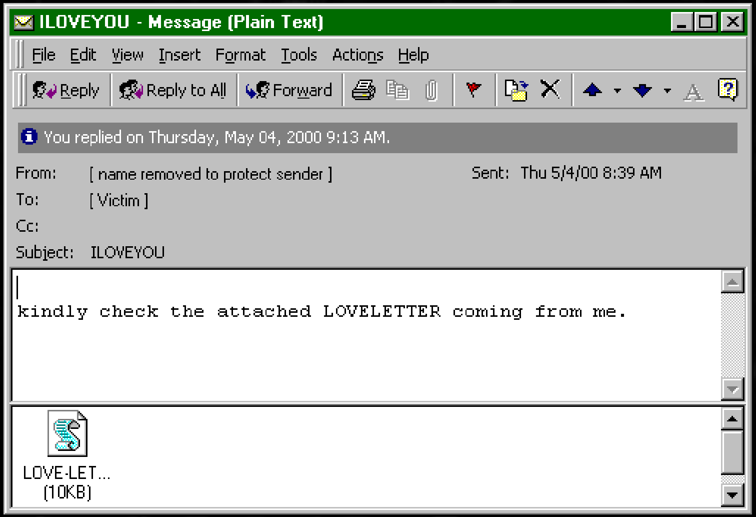

This website is very slow today!
Help, I can't accomplish any work!
Internet
I'll send so many pings that the server can't respond to anyone else.
ping
ping
ping
ping
WWW.XXYZCORP.COM
Web Server
DoS Attacker

- The goal was to clog the servers, and communication links on the way to the servers, so that useful traffic was gridlocked. The assault is not DNS-specific--the same attack has been used against several popular Web servers in the last few years.

- **DNS Amplification Attacks:** using publically accessible open DNS servers to overwhelm a victim system with DNS response traffic.

# DoS - Email Attacks

- When using Microsoft Outlook, a script reads your address book and sends a copy of itself to everyone listed there, thus propagating itself around the Internet.
- The script then modifies the computer's registry so that the script runs itself again when restarted.



ILOVEYOU - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

You replied on Thursday, May 04, 2000 9:13 AM.

From: [ name removed to protect sender ]

Sent: Thu 5/4/00 8:39 AM

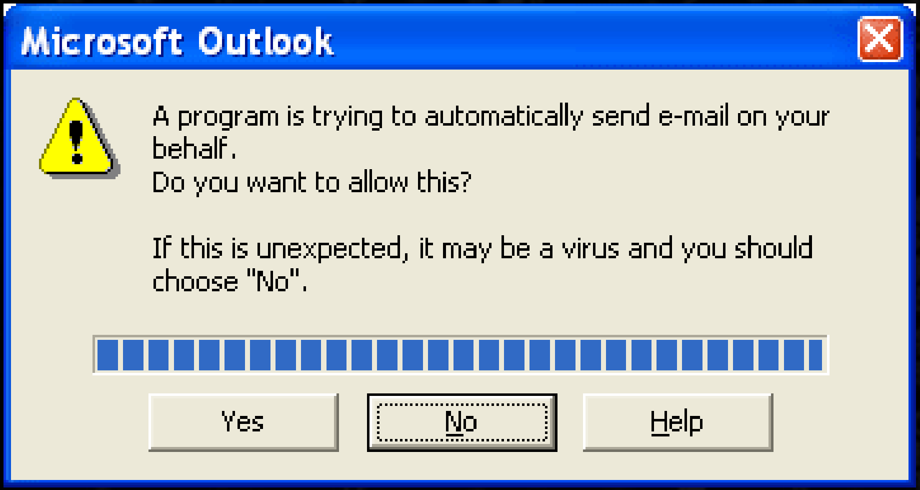
To: [ Victim ]

Cc:

Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LET... (10KB)



A program is trying to automatically send e-mail on your behalf.
Do you want to allow this?

If this is unexpected, it may be a virus and you should choose "No".

# DoS: Physical Infrastructure Attacks

- Someone can just simply snip your cables! Fortunately this can be quickly noticed and dealt with.
- Other physical infrastructure attacks can include recycling systems, affecting power to systems and actual destruction of computers or storage devices.

# DoS: Viruses/Worms

- Viruses or worms, which replicate across a network in various ways, can be viewed as denial-of-service attacks where the victim is not usually specifically targeted but simply a host unlucky enough to get the virus.
- Available bandwidth can become saturated as the virus/worm attempts to replicate itself and find new victims.

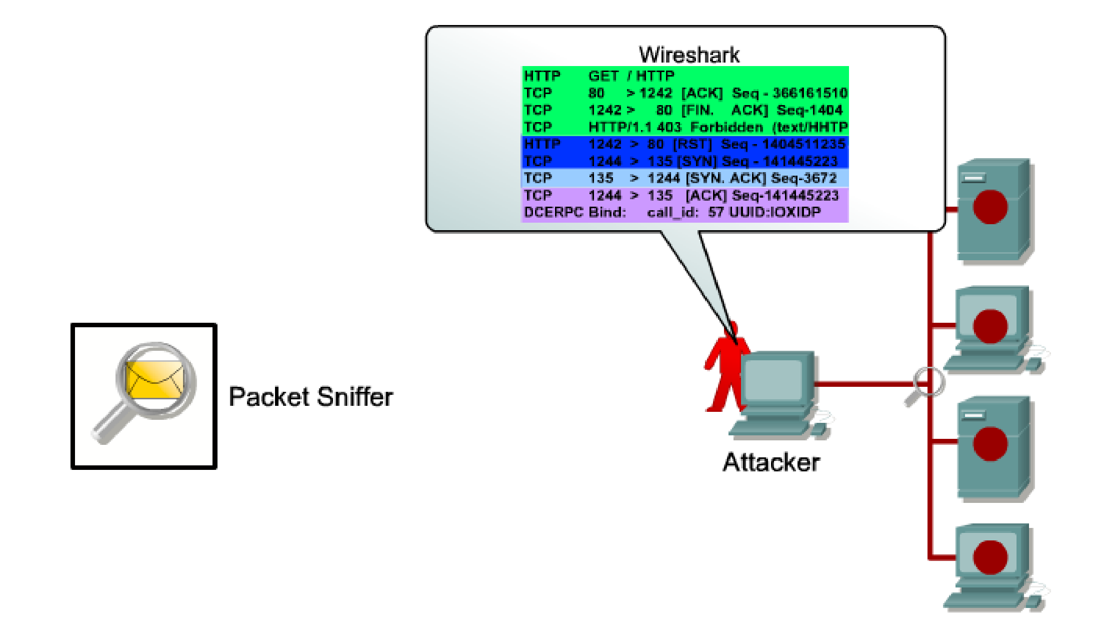
```
0 00 00-6D 73 62 6C        msbl
0 6A 75-73 74 20 77   ast.exe I just w
9 20 4C-4F 56 45 20   ant to say LOVE
                               illy
                               lo you
                               possi
                               makin
                               fix
                               re!!
```

# Malicious Code Attacks

- Refers to viruses, worms, Trojan horses, logic bombs, and other uninvited software
- Damage personal computers, but also attack systems that are more sophisticated
- Actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems
- Costs can be significant

Snap Stills/Rex Features

# Packet Sniffing Attacks



```
HTTP    GET  / HTTP
TCP     80    > 1242  [ACK]  Seq - 366161510
TCP     1242 >    80  [FIN.   ACK]  Seq-1404
TCP     HTTP/1.1 403  Forbidden  (text/HHTP
HTTP    1242  >  80  [RST]  Seq - 1404511235
TCP     1244  >  135 [SYN] Seq - 141445223
TCP     135    >  1244 [SYN. ACK] Seq-3672
TCP     1244  >  135   [ACK] Seq-141445223
DCERPC Bind:    call_id:  57 UUID:IOXIDP
```

- Most organization LANs are Ethernet networks
- On Ethernet-based networks, any machine on the network can see the traffic for every machine on that network
- Sniffer programs exploit this characteristic, monitoring all traffic and capturing the first 128 bytes or so of every unencrypted FTP or Telnet session (the part that contains user passwords)

# Information Leakage Attacks

- Attackers can sometimes get data without having to directly use computers
- Exploit Internet services that are intended to give out information
- Induce these services to reveal extra information or to give it out to unauthorized people
- Many services designed for use on local area networks do not have the security needed for safe use across the Internet
- Thus these services become the means for important information leakage

# Social Engineering Attacks

- Hacker-speak for tricking a person into revealing some confidential information
- An attack based on deceiving users or administrators at the target site
- Done to gain illicit access to systems or useful information
- The goals of social engineering are fraud, network intrusion, industrial espionage, identity theft, etc.

I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
scottadams@aol.com
www.dilbert.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFORMATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc.
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.

© Scott Adams, Inc./Dist. by UFS, Inc.

# Attack Methodology

**Stages** - the methodology of network attacks is well documented and researched. This research has led to greater understanding of network attacks and an entire specialization of engineers that test and protect networks against attacks (Certified Ethical Hackers/Penetration Testers)

**Tools** - penetration testers have a variety of power tools that are now commercially available. They also have may open source free tools. This proliferation of powerful tools has increased the threat of attack due to the fact that even technical novices can now launch sophisticated attacks.

# Stages of an Attack

- Today's attackers have a abundance of targets. In fact their greatest challenge is to select the most vulnerable victims.  This has resulted in very well-planned and structured attacks. These attacks have common logistical and strategic stages. These stages include;
  - Reconnaissance
  - Scanning (addresses, ports, vulnerabilities)
  - Gaining access
  - Maintaining Access
  - Covering Tracks

# Tools of the Attacker

- The following are a few of the most popular tools used by network attackers:
  - Enumeration tools (dumpreg, netview and netuser)
  - Port/address scanners (AngryIP, nmap, Nessus)
  - Vulnerability scanners (Meta Sploit, Core Impact, ISS)
  - Packet Sniffers (Snort, Wire Shark, Air Magnet)
  - Root kits
  - Cryptographic cracking tools (Cain, WepCrack)
  - Malicious codes (worms, Trojan horse, time bombs)
  - System hijack tools (netcat, MetaSploit, Core Impact)

# Countermeasures

- DMZ/NAT
- IDS/IPS
- Content Filtering
- Firewalls/proxy services
- Authentication/Authorization/Accounting (AAA)
- Self-defending networks
- Policies, procedures, standards guidelines
- Training and awareness

# Countermeasure Selection

- Cost /benefit calculation

  (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the company

- Evaluating cost of a countermeasure
  - Product costs
  - Design/planning costs
  - Implementation costs
  - Environment modifications
  - Compatibility
  - Maintenance requirements
  - Testing requirements
  - Repair, replacement, or update costs
  - Operating and support costs
  - Effects of productivity

# Network Security Jobs

- Network Security Administrator
- Risk Analyst
- VPN Specialist
- Penetration Tester
- Network Perimeter/Firewall Specialist
- Security Response IDS/IPS Engineer