The Cyber Threat

No Boundaries

Materials provided by:

Homeland Security

BARC*first*

Bay Area Response Coalition

Financial Industry Resilience, Security, and Teamwork

RPC*first*

REGIONAL PARTNERSHIP COUNCIL

This presentation was originally created by DHS in partnership with the Regional Partnership Council (RPC*first*) and the Bay Area Response Coalition (BARC*first)* to raise awareness and promote Public/Private Sector cooperation in the financial sector toward the prevention of, and response to, cyber threats of all types.

The original presentation has been customized by BARC*first* for presentation to other areas of the private sector.

Barry Cardoza

Chair, BARC*first*

Homeland Security

BARC*first*

Bay Area Response Coalition

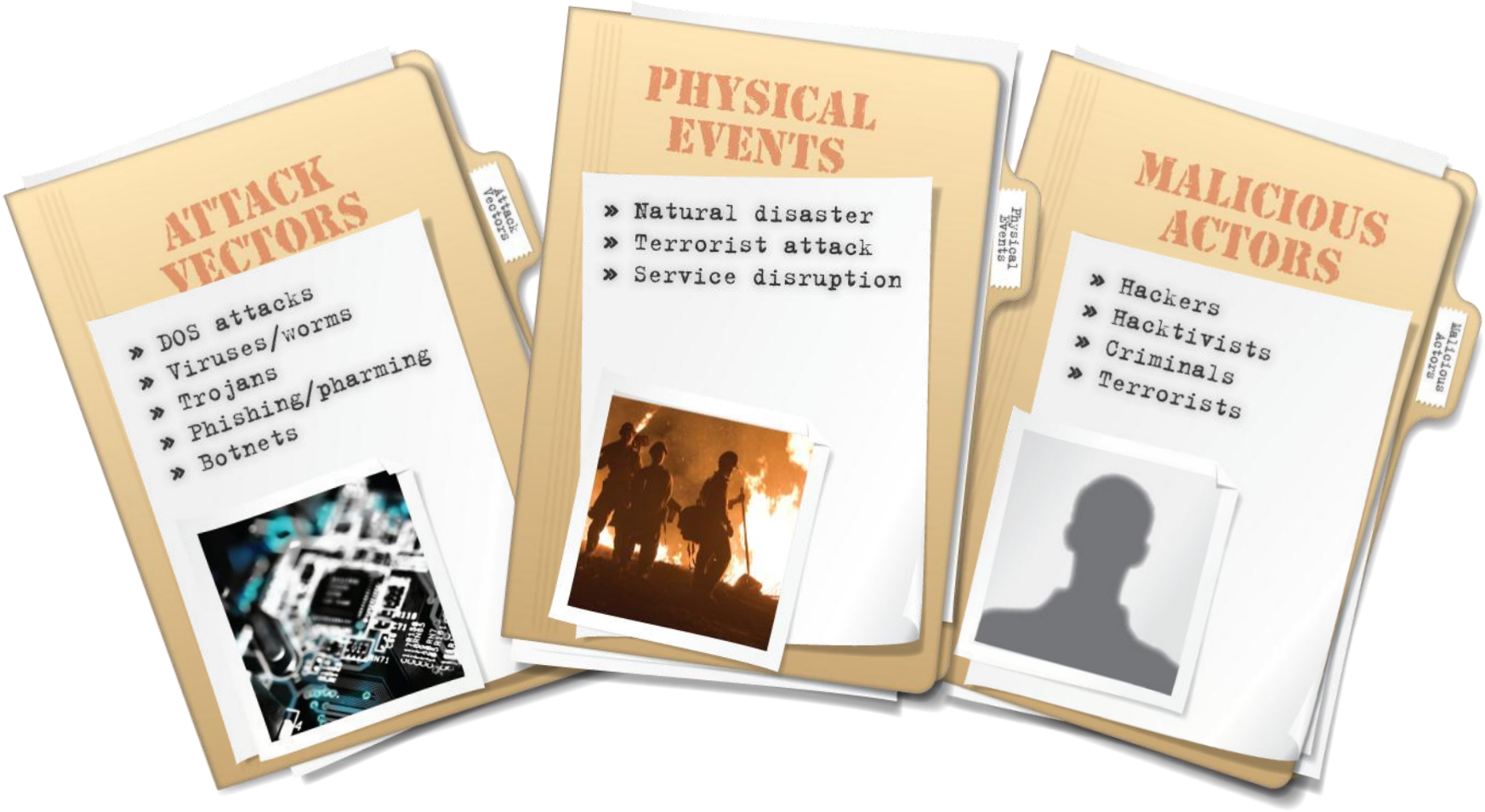
Financial Industry Resilience, Security, and Teamwork

RPC*first*

REGIONAL PARTNERSHIP COUNCIL

The Cyber Risk Landscape

Cyber incidents are increasing in frequency, scale, and sophistication.



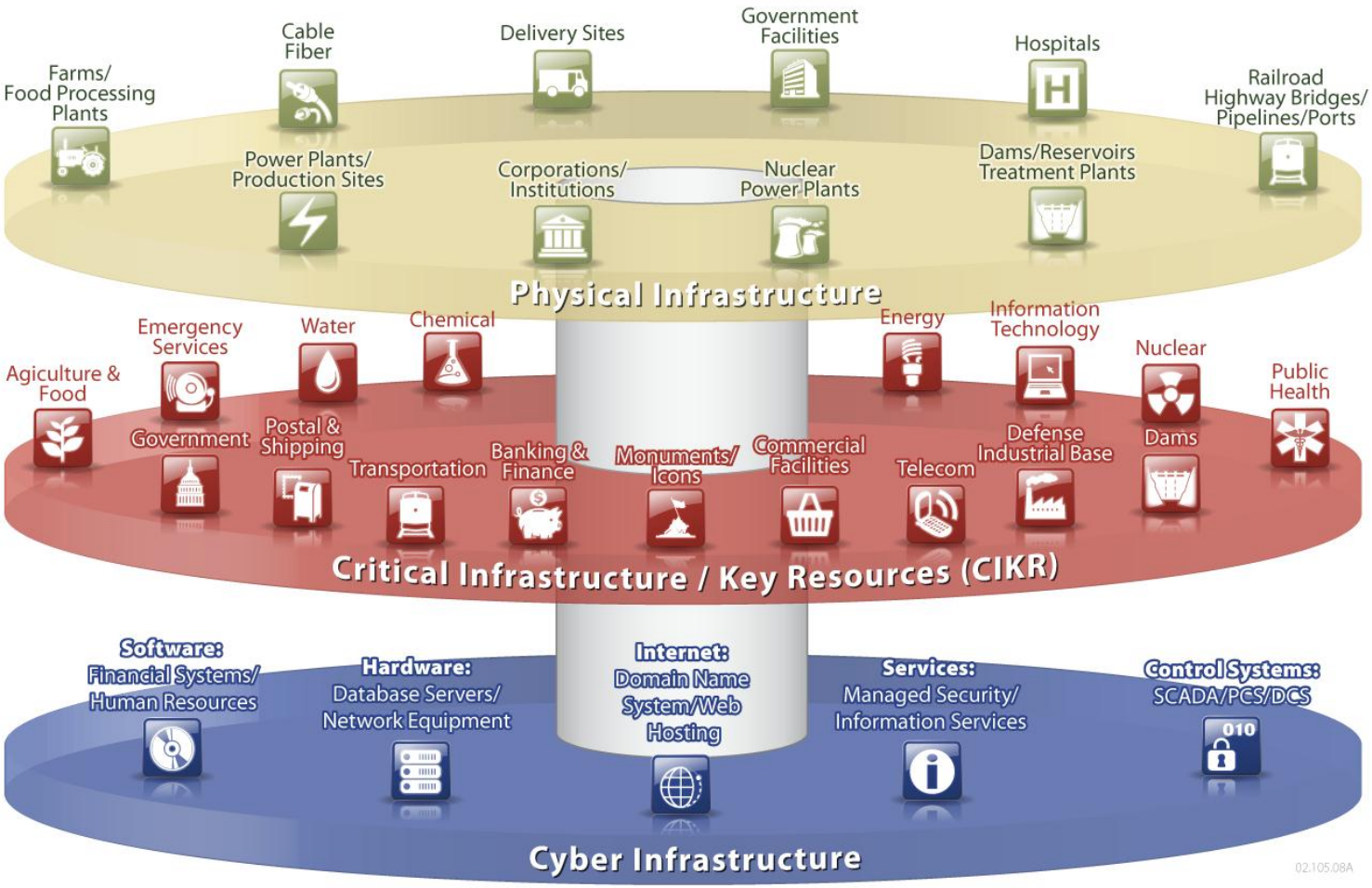
So, why is that?

The “Good Old” Days

Then

Now

Critical infrastructure depends on the vitality of the interwoven cyber infrastructure.



Exploitation of cyber vulnerabilities could carry serious consequences in the physical world.

- Interconnected and interdependent nature of the Internet raises risks for multiple sectors across unlimited geographic range
- Failure of or severe degradation to information technology sector or critical sector services could amplify cascading failures/stresses within various critical infrastructure
- A cyber incident could be coupled with a physical attack to disable emergency response, law enforcement capabilities, and Continuity of Operations/Continuity of Government contingencies
- Cyber incidents can severely impact business/service continuity in all sectors; cyber incidents typically affect the confidentiality, integrity, or availability of data transactions

Cyber-linkages among sectors raise the risk of cascading failures throughout the Nation during a cyber incident.

- The loss or degradation of certain critical infrastructure functions could negatively impact performance in other areas
- The private sector owns over 80% of the critical infrastructure; during an incident, the private sector is often first to detect a problem
  - For example, a successful cyber attack on a power plant's control system could impact several critical sectors, as detailed below:

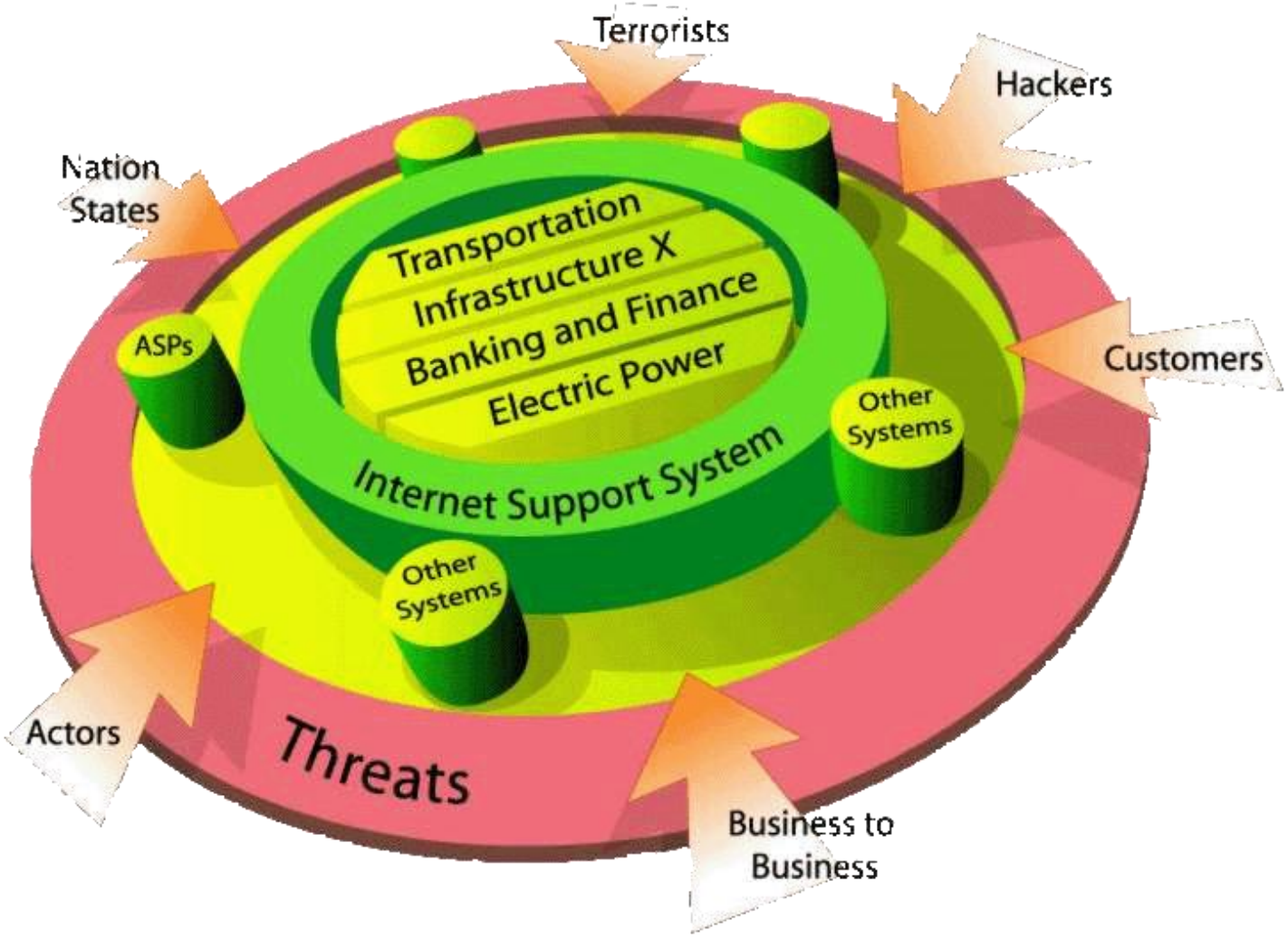
Electric Power Sector

Communications Sector

Emergency Response

Financial Sector

Convergence



What are our Threats today?

- Natural Disasters
  - Earthquakes
  - Floods
  - Tornados
  - Hurricanes
  - Etc.

What are our Threats today?

- Accidents & Failures
  - Hardware Failure
  - Human Error
- Terrorism
  - International
  - Domestic

FIRE

Seattle data center fire knocks out Bing Travel, other Web sites

by Cook, Bishop on Friday, July 3, 2009, 7:07am PDT
52 Comments | Permalink
Bad news | Broadband | Business | Corporate IT | Web

http://www.techflash.com/seattle/2009/07/Seattle_data_center_fire_knocks_out_Bing_Travel_other_Web_sites_49876777.html

Data center tenants carry servers out of Fisher Plaza this morning.

What are our Threats today?

- Script Kiddies
- Criminals
- Industrial Espionage
- Insiders
- Foreign Governments

Several Attacker Profiles

- **Insiders**
  - Insiders have a unique advantage due to access/trust
  - They can be motivated by revenge, organizational disputes, personal problems, boredom, curiosity, or to “prove a point”

- **Script Kiddies**
  - Relatively untrained hackers that find exploit code/tools on the Internet and run them indiscriminately against targets
  - While largely unskilled, they are numerous

- **Criminals**
  - Cyber based attacks offer new means to commit traditional crimes, such as fraud and extortion
  - Organized cyber crime groups have adopted legitimate business practices, structure, and method of operation

- **Terrorists**
  - Cyber attacks have the potential to cripple infrastructures which are not properly secured
  - In addition, cyber-linkages between sectors raise the risk of cascading failures throughout the Nation

Web security is becoming more difficult…

- Interactive abilities of Web 2.0 have led to an abundance of new applications; these coupled with insecure coding practices have led to a constantly evolving set of security concerns and vulnerabilities
- Many websites are vulnerable to:
  - **Defacement**
  - **SQL Injection**
  - **Spoofing Attacks**
  - **Cross-Site Scripting (XSS)**
- Like any new technology, attackers are currently targeting IPv6 services, and capitalizing on a lack of understanding

Common attack methods pose serious risks to Critical Infrastructure Key Resources (CIKR)

Distributed Denial of Service (DDoS) Attack	Web Application Vulnerabilities	Data Theft
▪ Occurs when an attacker floods a system server with data from multiple computers ▪ Results in disruption of network services	▪ Structured Query Language (SQL) Injection, Cross Site Scripting (XXS), etc. are increasingly common ▪ Visitors to an infected site are susceptible to malware and/or loss of personnel information	▪ Occurs through proliferation of malware, spyware, as well as social engineering ▪ Lack of international legal framework results in attacks generated from other nations
DNS Cache Poisoning	**Botnets**	**Control System Risks**
▪ Involves corrupting records on a Domain Name System (DNS) server, so that a resolver will return the Internet Protocol (IP) address of an incorrect/ compromised domain	▪ A series of compromised systems running malicious software, from which an attack can be orchestrated ▪ Oftentimes, users do not even realize they are part of the botnet	▪ Modems are prevalent in the Control System environment – often used for remote access to field equipment ▪ As Smart Grid deployment begins, wireless connections will continue to be a concern

Critical infrastructure is crucial to National Security

Estonia attacks, April 2007 **:**

- A series of denial-of-service attacks which overwhelmed Estonian government, banking, and broadcaster websites in April 2007
- Attacks occurred during a public dispute with Russian government. Russian sympathizers within Estonia eventually claimed responsibility for the attacks

Poland transit incident, January 2008 :

- Using an Internet connection and a modified television remote, a 14 year old boy took control of the light-rail system in the city of Lodz
- The attack on the systems command and control systems resulted in the derailment of four trains

Russian – Georgian War, August 2008:

- Distributed denial-of-service attacks (DoS) crippled many Georgian Web Sites
- Georgian officials alleged the coordinated cyber attacks against their Web Sites were conducted by Russian criminal gangs tipped off about Russia's intent to invade
- Hackers appeared to have been prepped with target lists and details about Georgian web site vulnerabilities before the two countries engaged in a ground, sea, and air war

Cyber Crime and Theft

- E-crime “has become a major shadow economy ruled by business rules and logic that closely mimics the legitimate business world”
- Cyber criminals target commercial organizations for:
  - **Personal Data of Customers and Employees**
  - **Finances (through theft or extortion)**
  - **Proprietary Data/Industrial Espionage/Intellectual Property**
- From January 1, 2008, through December 31, 2008, there were 275,284 complaints filed online with Internet Crime Compliant Center (IC^3) – a 33.1% increase from the previous year
- The U.S. Department of Commerce estimates stolen Intellectual Property costs companies a collective $250 billion each year

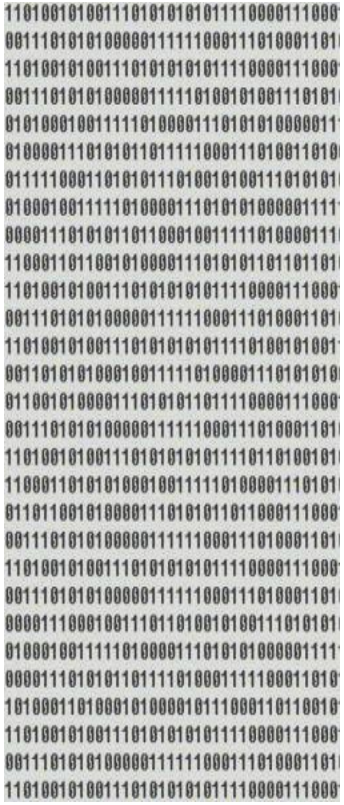
Financial Sector Highlights

- The financial sector was the top sector for identities exposed in 2008, accounting for 29 percent of the total, an increase from 10 percent in 2007

- Attackers are concentrating on compromising end users for financial gain. In 2008, 78 percent of confidential information threats exported user data, and 76 percent used a keystroke-logging component to steal information, such as online banking account credentials

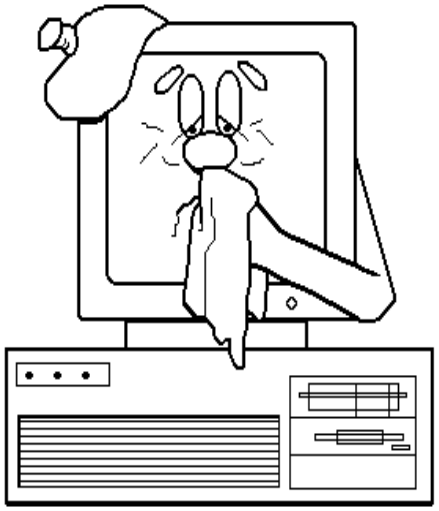
- 76 percent of phishing lures targeted brands in the financial services sector; this sector had the most identities exposed due to data breaches

Malware



- Malware can be hosted on malicious websites, sent via email, or made to self-propagate across networks
- It can be used to steal information, destroy data, annoy users, or allow attackers to remotely control hosts
- Common types include:
  - Virus
  - Worm
  - Trojan

Malware



- **Virus** - (Ex. Melissa)
  - Malware that is parasitic in nature and replicates by copying itself to other programs;
  - Not able to self-replicate, requires an executable
- **Worm** - (Ex. ILOVEYOU, Code Red)
  - Causes maximum damage to corporate information
  - Self-replicates across networks, without a host file, through inbuilt email or scan engines
- **Trojan** - (Ex. Bowling for Elves)
  - An “impostor,” a program that appears legitimate, but contains malicious code, and does not self-replicate
  - Can be a carrier for a virus

Botnets and Denial of Service (DoS) Attacks

- Botnets are massive pools of compromised computers used to send out spam and viruses, host scam web sites, harvest information, and disrupt or block internet traffic
- The United States was the country most frequently targeted by denial-of-service attacks in 2008, accounting for 51 percent of the worldwide total
- Threats to computer and cyber systems show no signs of decreasing. The FBI has identified more that 2.5 million computers as under control of global “botnets”
- DoS attacks are particularly threatening for any institution that conducts important business transactions online, including financial settlements or just-in-time operations

* Arbor Networks

Sample Scenario

Today is July 27…

- On Patch Tuesday, Microsoft releases four patches. All are ranked "critical."
  - **The bulk of the vulnerabilities addressed by fixes today could be exploited if a Windows user simply visits a malicious web site… criminals are increasingly using the Web to deliver malicious software.**
  - **In such drive-by downloads an attacker places malware onto a vulnerable computer without the user noticing it.**

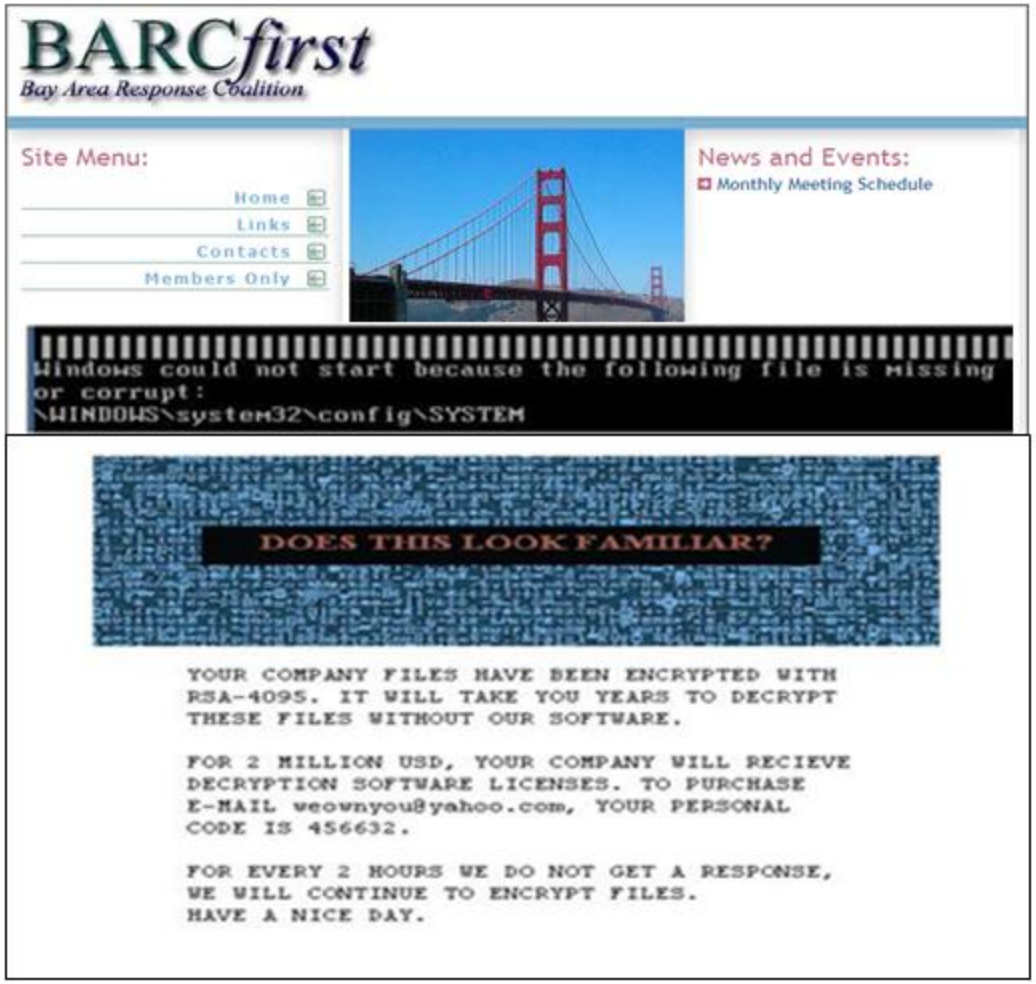
Does your company (and you on your home equipment) install these patches as soon as they are released?

If not, since more of the "bad guys" *now know* about these vulnerabilities, and you are in *increased* danger.

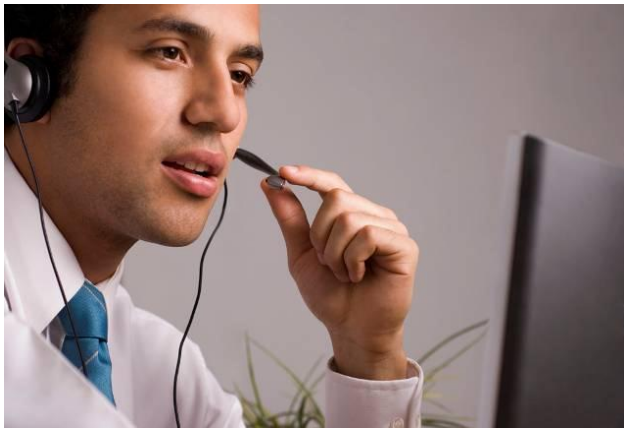
BARC*first* Alert Email

- On July 27, BARC*first*
  receive an alert email f
  BARC*first* Steering Co
- The email reports on a
  shooter in the downtov
- It also contains an atta
  an embedded link for a
  most up to date inform

BARC*first* website defaced

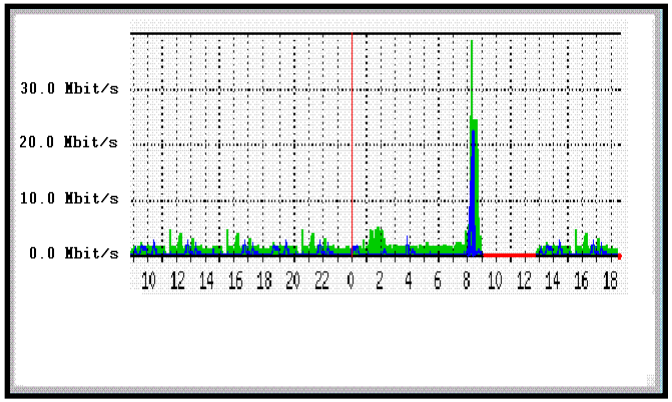


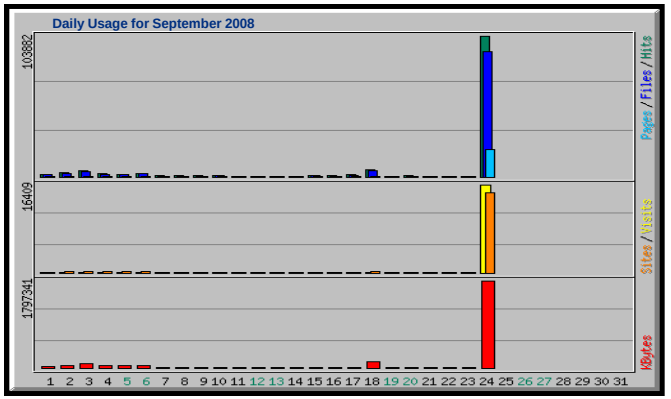
Initial Reports…



- Your organization is reporting that Help and Technical Support Desks are receiving a significant volume of calls

Technical Investigation…



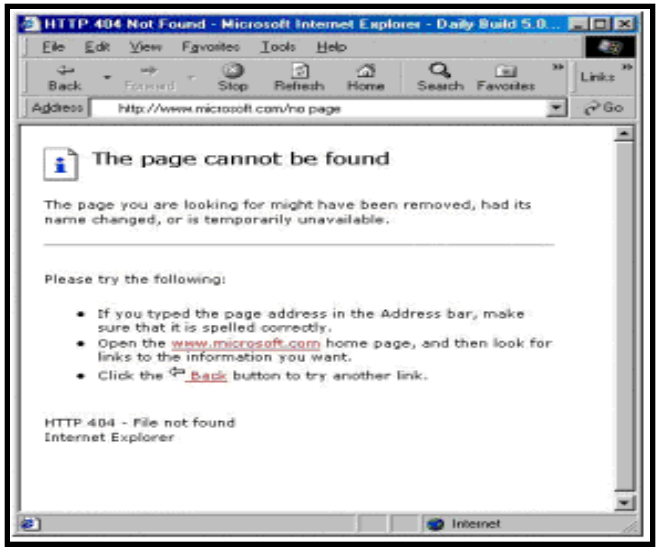


Charts Depicting Network Traffic

- Technical personnel evaluate the situation and determine they are experiencing an extreme spike in network traffic - completely consuming bandwidth
- Your organization is under a distributed denial-of-service attack

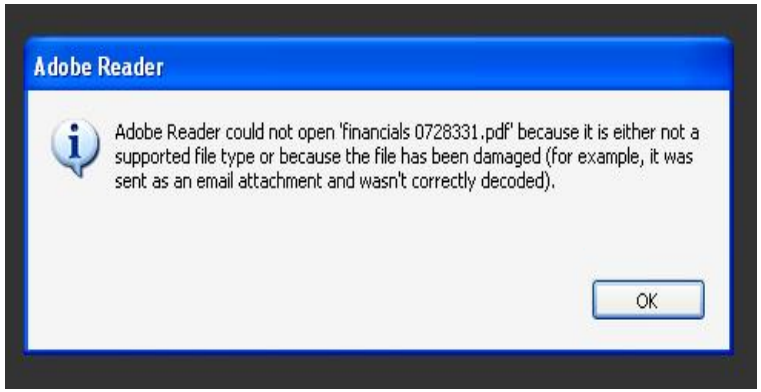
Developing Situation…

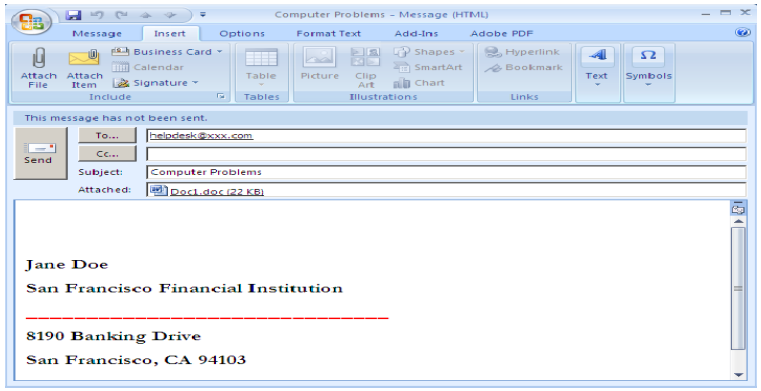
- Later that afternoon, Help Desks/Technical Support Groups are once again flooded with calls…



- Complaints Include:
  - **External users, employees, and customers attempting to access company websites see error code HTTP 404, "The page cannot be found"**
  - **Emails sent to/from external networks do not go through**
  - **Internal network resources are sluggish**
  - **Operations are being affected noticeably**

And, now far worse…





- Internal Users are reporting:
  - **Inability to access their important files (including .doc, .pdf, and .xls files)**
  - **Suspicious attachments of varying file formats that do not open properly**
- These are problems that could begin to affect firm operations

Problems Continue…

- The problem is becoming more severe over time, with more user complaints and greater consequences for business operations
  - **Compromised machines and files are multiplying**
  - **Help Desk/Tech Support Groups are overwhelmed**

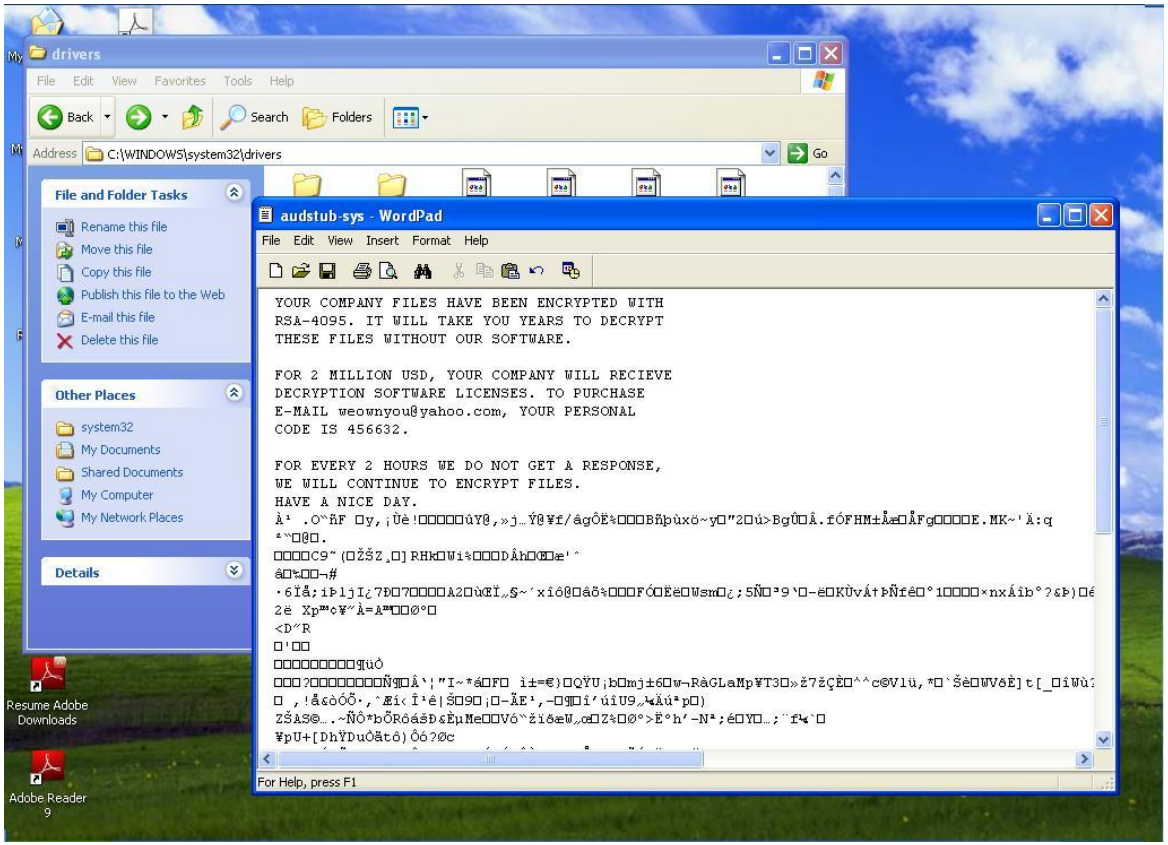
Initial Assessment…

- Help and Technical support desk staff have found:
  - **Various user files that have been changed to encrypted .txt files**
  - **Malicious attachments circulating through the network via email**
- Typical troubleshooting approaches are unsuccessful

Screenshot of encrypted .txt file

Developing Situation…

- Shortly after lunchtime, technical personnel report finding a variation of this note in many of the encrypted .txt files:



Decision Time…

- Technical personnel pass along the information to company/organization decision makers who must decide on a course of action

Your company files are encrypted with RSA-4096 algorithm. You will need years to decrypt these files without our software.

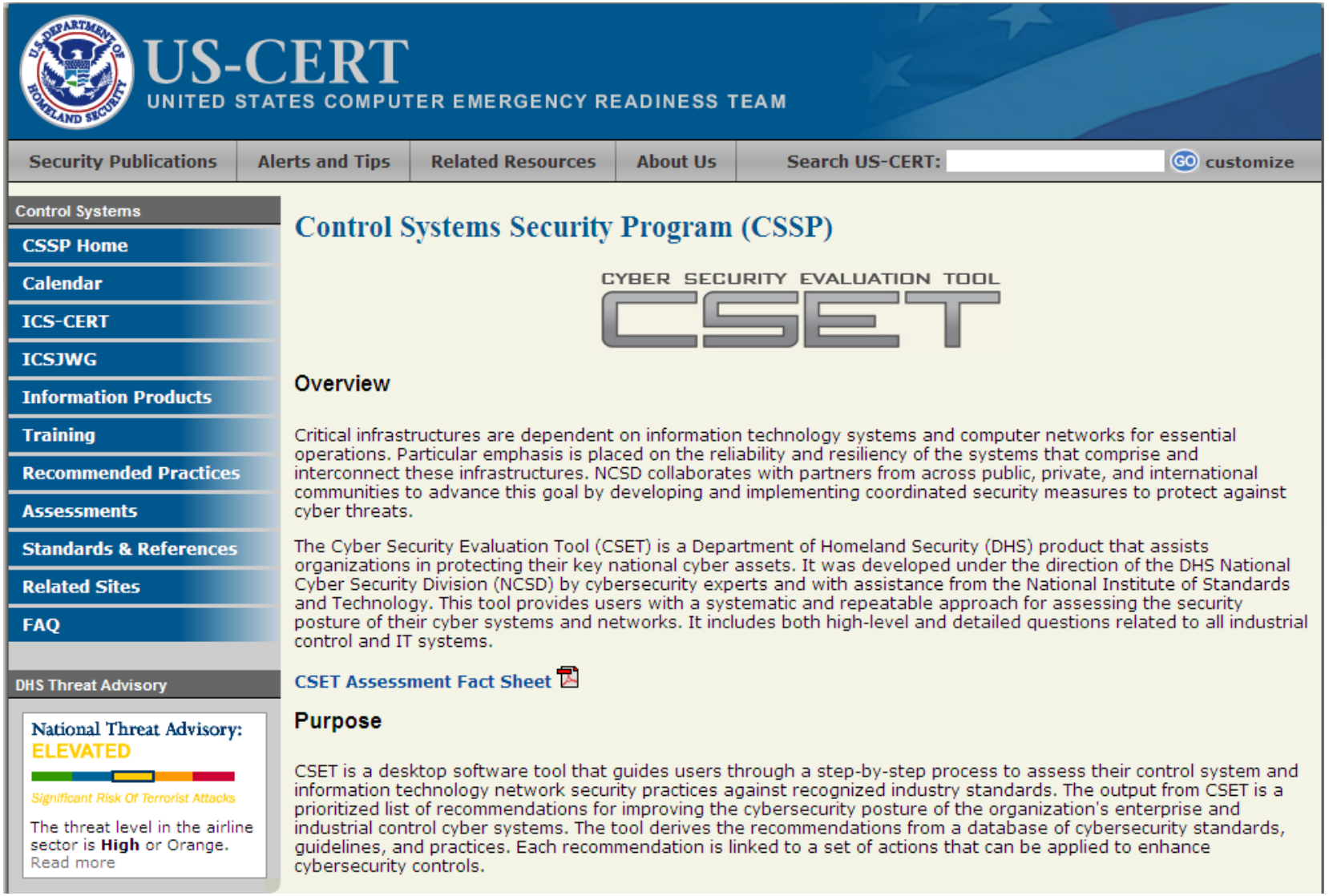
For 2 million USD, your company will get decryption software licenses. To purchase, email weownyou@yahoo.com, your personal code is 29583

For every 2 hours we do no get a response you will also experience a distributed denial-of-service attack.

Have a nice day.

KEY POINT

The government may not know that a sector-focused, regional, or even national attack is occurring if businesses do not report that they are being attacked.



To learn more, visit http://www.us-cert.gov/control_systems/satool.html .

CSET is available in DVD format. To obtain a DVD copy of CSET, send an e-mail with your mailing address to CSET@dhs.gov.

Questions?

Join us on June 9th when we will be talking about what individuals can do to help protect themselves from the Cyber Threat.

Homeland Security