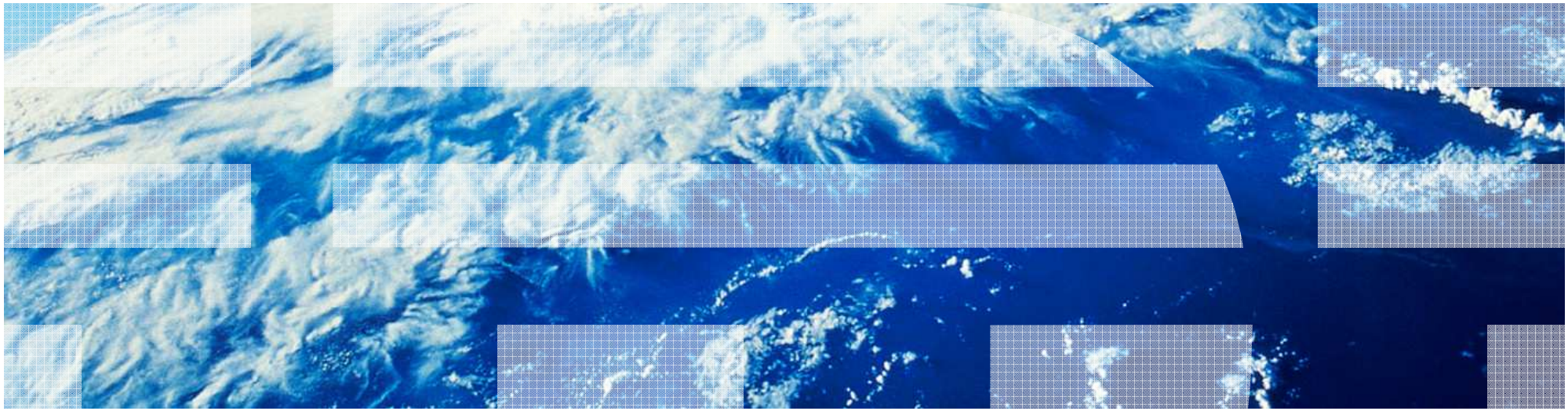
Emergency Response Service



Who is our team

- **The Cyber Security Intelligence and Response team is staffed with:**
  - Highly skilled forensic analysts and consultants dedicated to incident response.
  - Resident malware specialists who research malware trends and perform malware breakdown and behavioral analysis.
  - Application security experts who can proactively identify existing vulnerabilities in applications in any phase of the software development life cycle and can work with clients to improve security within the life cycle.
  - Highly skilled penetration testers that can identify potential weaknesses and threats within your network or applications and on any platform.

- **All members of this team average 10 years of experience in the security field and hold several recognized security certifications.**

IBM Emergency Response Service – Who We Are

- As part of the world-renowned IBM X-Force security intelligence organization, the IBM Emergency Response Service team delivers unparalleled service by combining market-leading IBM X-Force security research with real-world incident response experience.

IBM Emergency Response Service – Client Types

- Types of subscription clients globally:
  - **Oil and Gasoline**
  - **Banking and Financials**
  - **Retail**
  - Utilities
  - **Automotive / Transport**
  - **Government**
  - **Computer and Electronics**

  - Education
  - **Law**
  - Insurance
  - Travel
  - **Manufacturing**
  - Entertainment
  - Health Care
  - **Security**

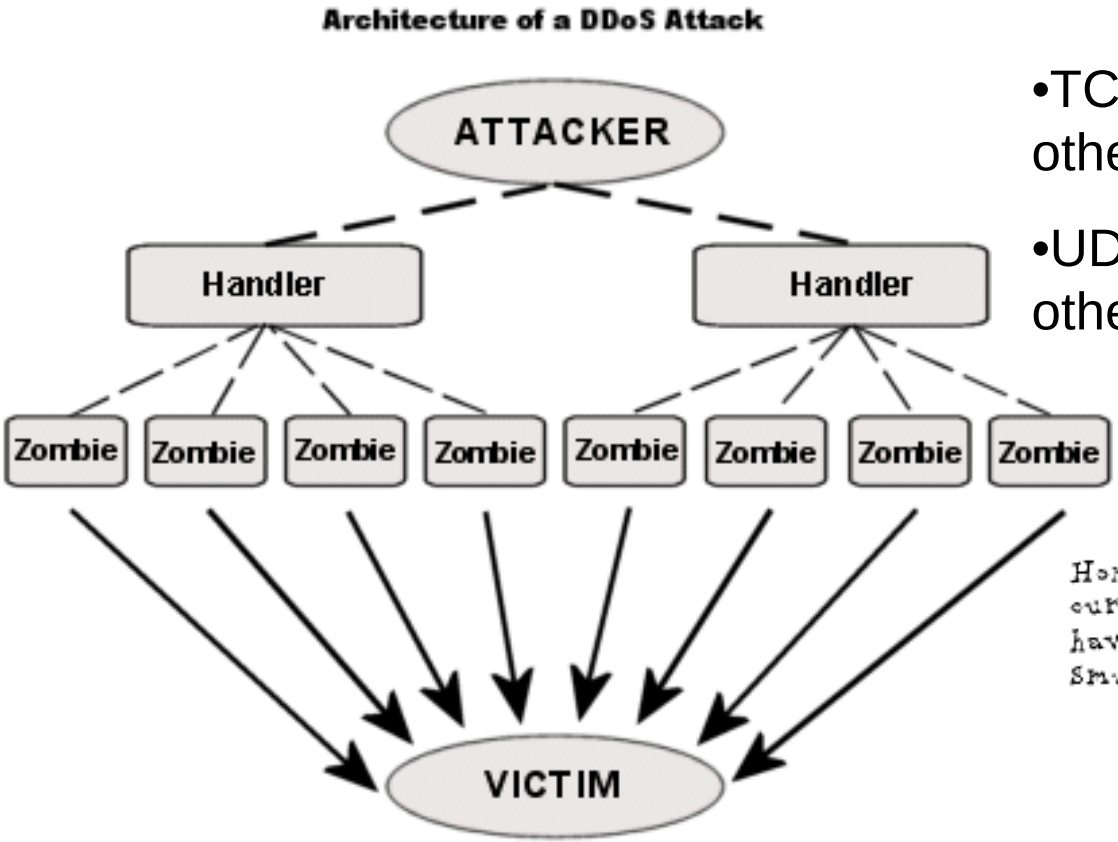
- We also have an “ad-hoc” service, for those that haven’t signed up to the subscription service…

Customer “Real World” Incidents

- Military Contractor – Hacked and New Malware
- Security Company – Hacked
- Gas Company – Malware Outbreak
- Bank – DDoS
- Bank – Hacked
- Bank – Hacked and Extortion
- Oil Company – Malware Outbreak

- Shipping Company – Multiple Malware Outbreaks
- Mobile Telephone Network – Insider Misuse
- Bank – Insider Misuse
- Police Force – Malware Outbreak

Distributed Denial of Service (DDoS)



- TCP (SYN, Connect) Flood, and others
- UDP Flood (Fraggle Attack) amongst others

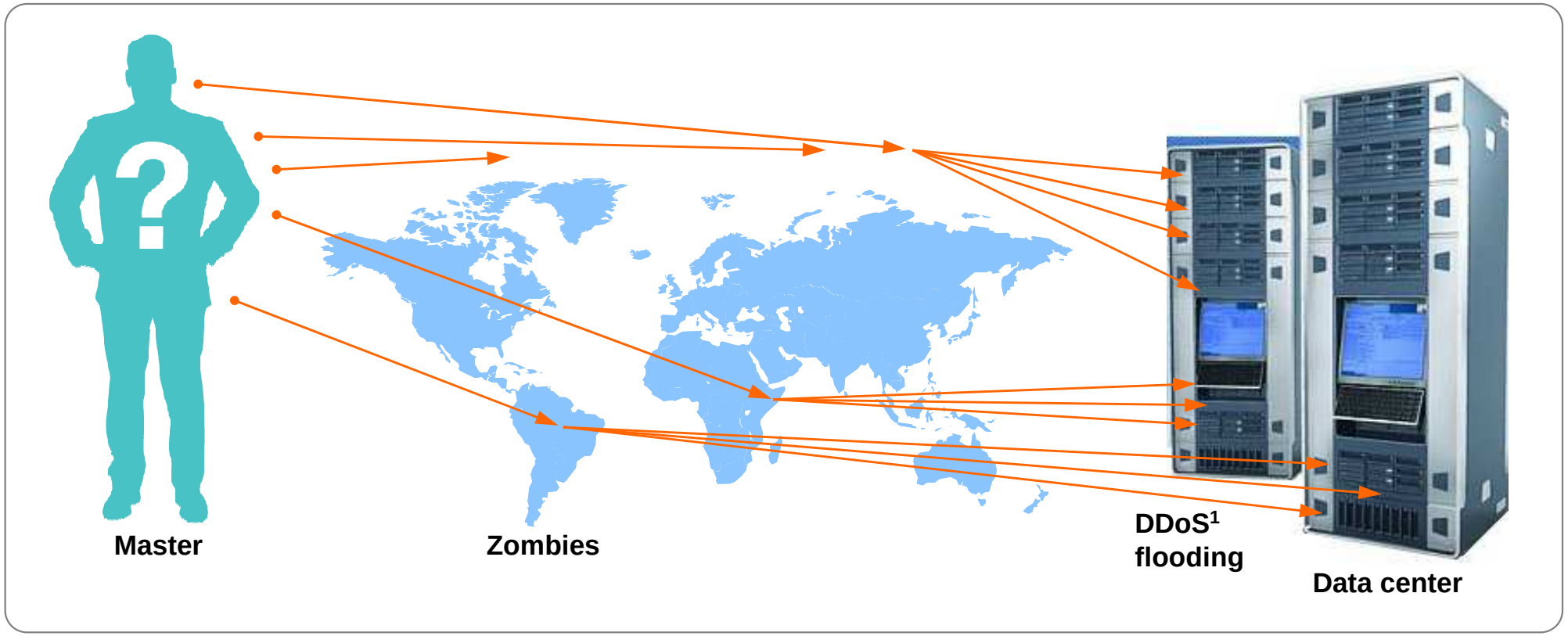
- ICMP (Ping Flood) aka “Smurf Attack”
- Lots of other DoS and DDoS methods
- Easy and cheap to carry out, just need willing volunteers or a Botnet…

Here is the anatomy of a denial-of-service attack.

Hacktivist or other adversary launches concurrent attacks from multiple worldwide locations

Attacks intended to saturate network connections and disable web presence

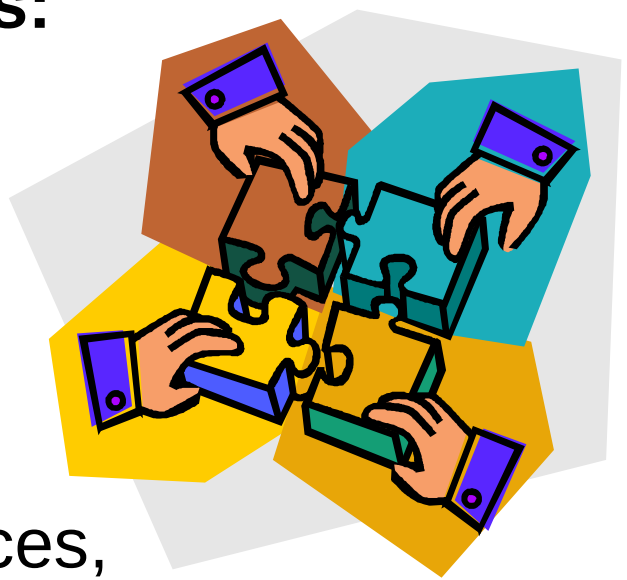
Results in lost business opportunities and brand impact



[1]Distributed denial of service (DDoS)

IBM Emergency Response Service – Subscription Overview

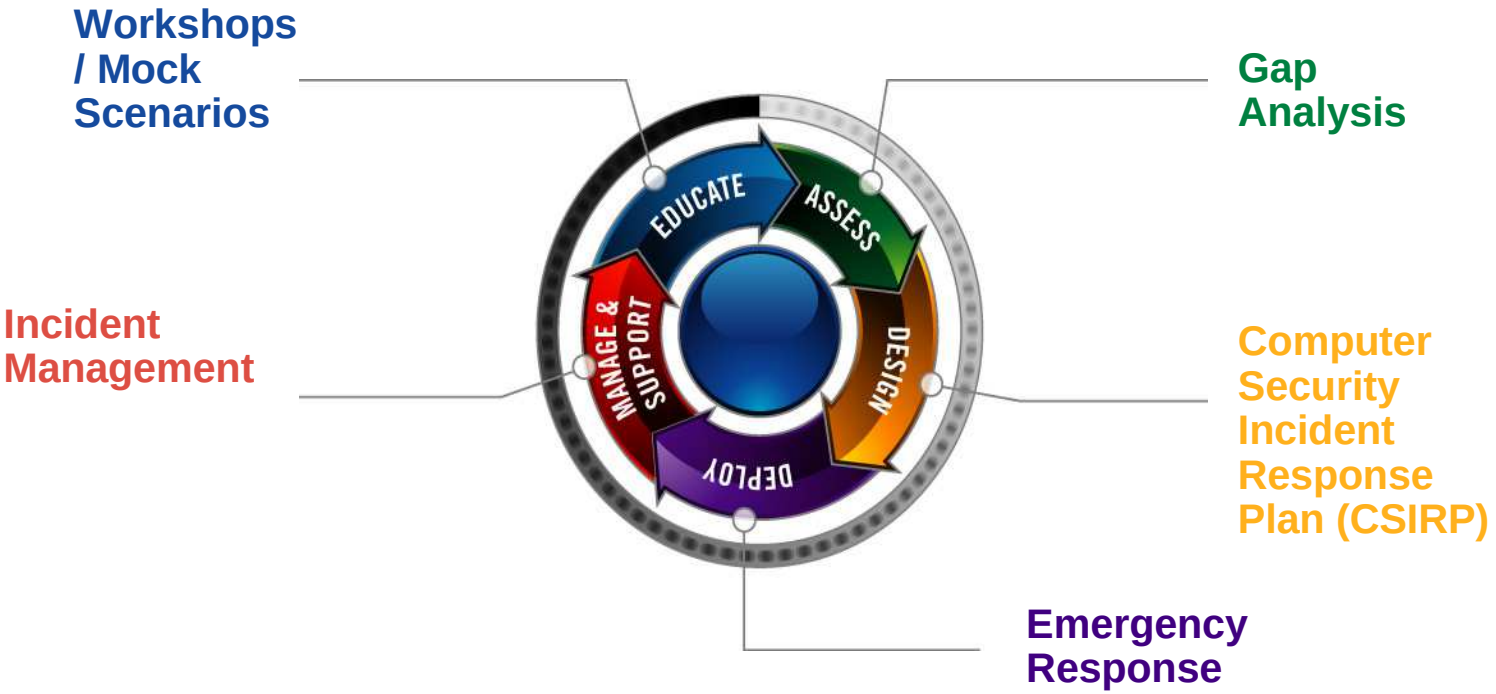
- **A Subscription is simply a service that allows our customers to retain expert consultants prior to the occurrence of an incident and covers:**



  - Emergency Response
  - Incident Management
  - Incident Analysis
  - Data Collection and Preservation
  - Detailed Data Analysis (Mobile Devices, Computers, Networks and Enterprise Forensics)

IBM Emergency Response Service – Subscription Overview

- **In order for us to accomplish this mission, we provide the following services:**



IBM Emergency Response Service – Subscription Overview

- **The following services are included with the Subscription:**
  - On-site kick-off and service preparation (one day, one person)
  - Unlimited Emergency Incident Declarations per year (consisting of one physical Customer location, within the country in which the Services are being contracted)
  - 120 Staff Hours per year (On-site and/or Remote)*
  - Unused hours by month 9 may be used towards: Malware defence review, Incident response training and development, etc.
  - 1 annual onsite (8 hrs) for incident planning, gap analysis, or mock scenarios
  - X-Force Threat Analysis Service (2) Seats (additional seats can be purchased)
  - Discounted Staff Hourly rate per hour after the initial 120 hours are used up

* Unused annual staff-hours DO NOT roll over into subsequent contract years.

IBM Emergency Response Service – Subscription Overview

- **On-site Kick-off and Service Preparation**
  - Introduces the personnel providing the Services
  - Confirms customer location to be included in the Services
  - Defines the process for making an Emergency Incident Declaration, including establishing the designated telephone numbers and email addresses
  - Review processes for responding to an Emergency Incident Declaration and for exchanging security Incident data in a secure manner.
  - Review questionnaires or other input sheets provided by IBM; and
  - Discuss risk tolerance and other issues, as applicable

IBM Emergency Response Service – Incident Declarations

- **IBM Emergency Response Service will provide on site and/or remote assistance and advice if possible for handling the Emergency Incident Declaration including:**
  - Analysis of computer security incident data to determine the source of the incident, its cause, and its effects;
  - Assist in preventing the effects of the computer security incident from spreading to other computer systems and networks;
  - Assist with stopping the computer security incident at its source and/or protecting Customer's computer systems and networks from the effects of the computer security incident;
  - Recommendations for restoration of the affected computer systems and networks to normal operations; and
  - Suggesting protection methods for Customer's computer systems and networks from future similar occurrences

IBM Emergency Response Service – Annual Staff Hours

- **Optionally, unused annual staff-hours may be applied towards one of the following within the 4th Quarter of each contract year:**
  - On-Site Incident Preparedness Visit*
  - Workshop* (First Responder Responsibilities, Mock Incident Drills)
  - High-Level CSIRP Review (Inadequate or missing Industry Best Practices, etc.

* On-Site Incident Preparedness Visits / Workshops require three staff hours preparation time for every staff hour on-site.

Incident Response Program Development and Gap Assessment

When an incident occurs, businesses need the right **process, tools, and resources** to respond and minimize impact

Being prepared to minimize the impact of a security incident and to recover faster

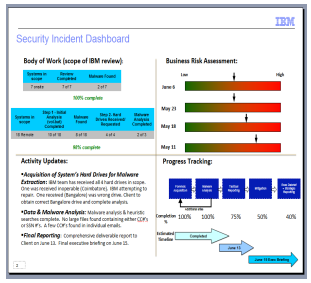
Protecting critical systems and data from downtime and/or information theft

Analyzing the root cause of an incident and preventing its spread

Restoring affected systems to normal operations

Preventing similar incidents from causing future damage

Meeting regulatory compliance requirements for incident response



The **Incident Response Plan is the foundation** on which all incident response and recovery activities are based

It specifically defines the organization, roles and responsibilities of the Computer Security Incident Response Team (CSIRT)

It should have criteria to assist an organization determine what is considered an incident versus an event

It defines escalation procedures to management, executive, legal, law enforcement, and media depending on incident conditions and severity

The plan and process should be fully tested via dry runs and incident mock tests

A well-developed plan provides a framework for effectively responding to any number of potential security incidents

Test Approach

Potential Cyber-security test focus areas:

Step 1: Prevention *– Effectiveness at stopping attacks at the perimeter*

Penetration Test (not just a vulnerability scan!)
Application Test (test all the systems that customers and partners can access)
Test all your security defences (firewalls, IPS/IDS, AV, DoS/DDoS, etc.)
Test your staff; Phishing, Tailgating, Secure Disposal, USB Sticks, Social Engineering…

Step 2: Detection *– Effectiveness at discovering what is already in the perimeter*

Do they have access, can data be extracted, have backdoors been planted?
Perform a controlled test to detect if a malware infection is growing
Perform a controlled test to detect irregular transmission of data or inter-enterprise communications

Step 3: Incident Response

Step 3a: Containment *– Effectiveness at isolating or stopping cascading within the enterprise*

Test capabilities to prevent a malware Infection from spreading

Step 3b: Remediation *– Effectiveness at returning critical capabilities*

can we restore client capabilities
can we remediate a large number of infected laptops or network equipment

Step 4: Learn from the Incident

Carry out a root-cause analysis
Understand what worked and what didn't during the incident
Apply the knowledge to help minimise a similar attack, or at least to improve your readiness for the next one… It will happen!

IBM Emergency Response Service – XFTAS Seats

- Each subscription includes two (2) built in seats to the XFTAS.
- XFTAS is a security intelligence service that delivers customized information about a wide array of threats that could affect your network security.
- XFTAS helps you proactively protect your networks with detailed analyses of global online threat conditions.
  - A single source for up-to-the minute, customized security information
  - Expert analysis and correlation of global security threats
  - Actionable data and recommendations that help you maintain your network security
  - Partnership with a trusted security advisor

Example screen shots can be found at the end of this presentation