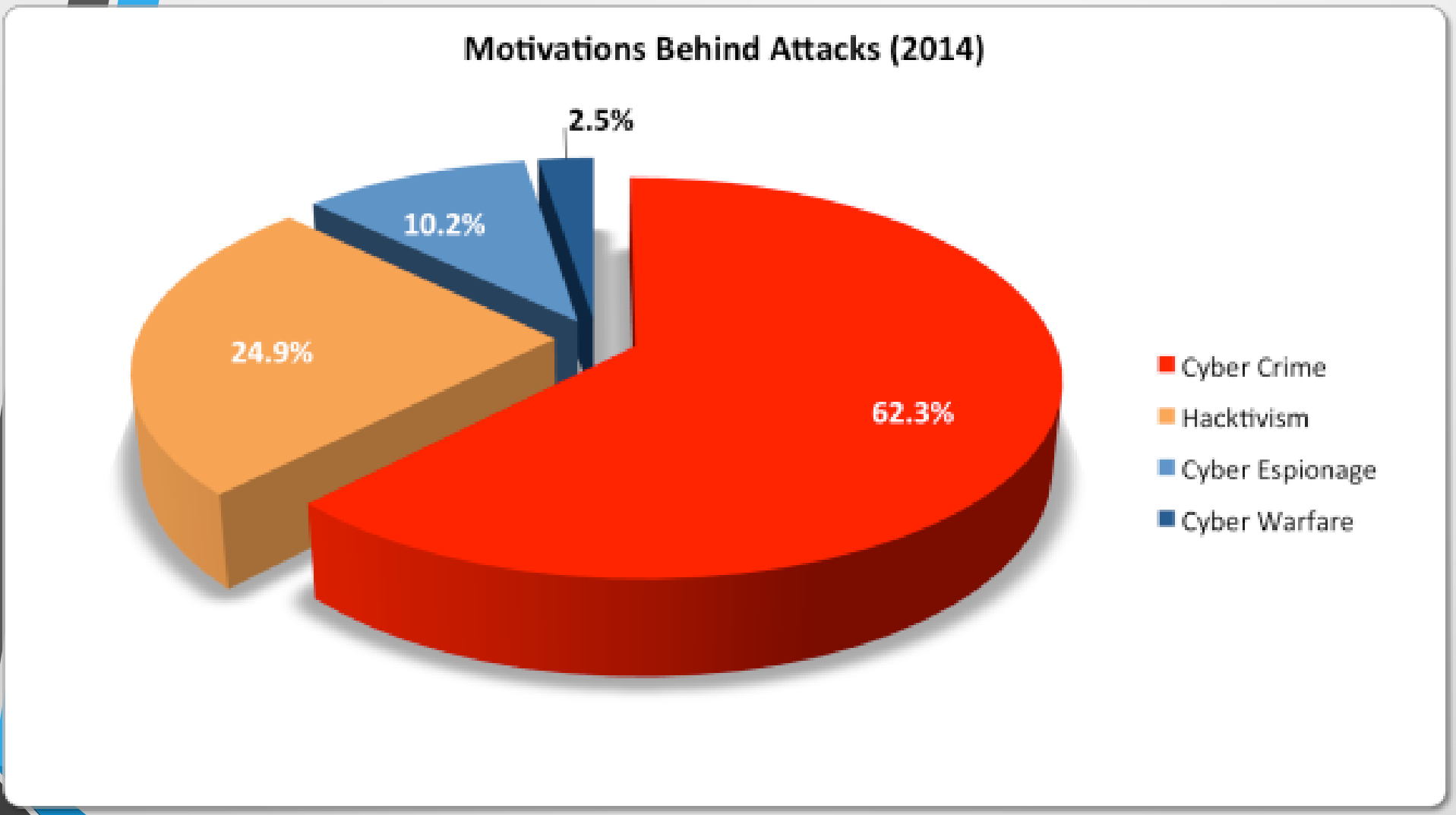
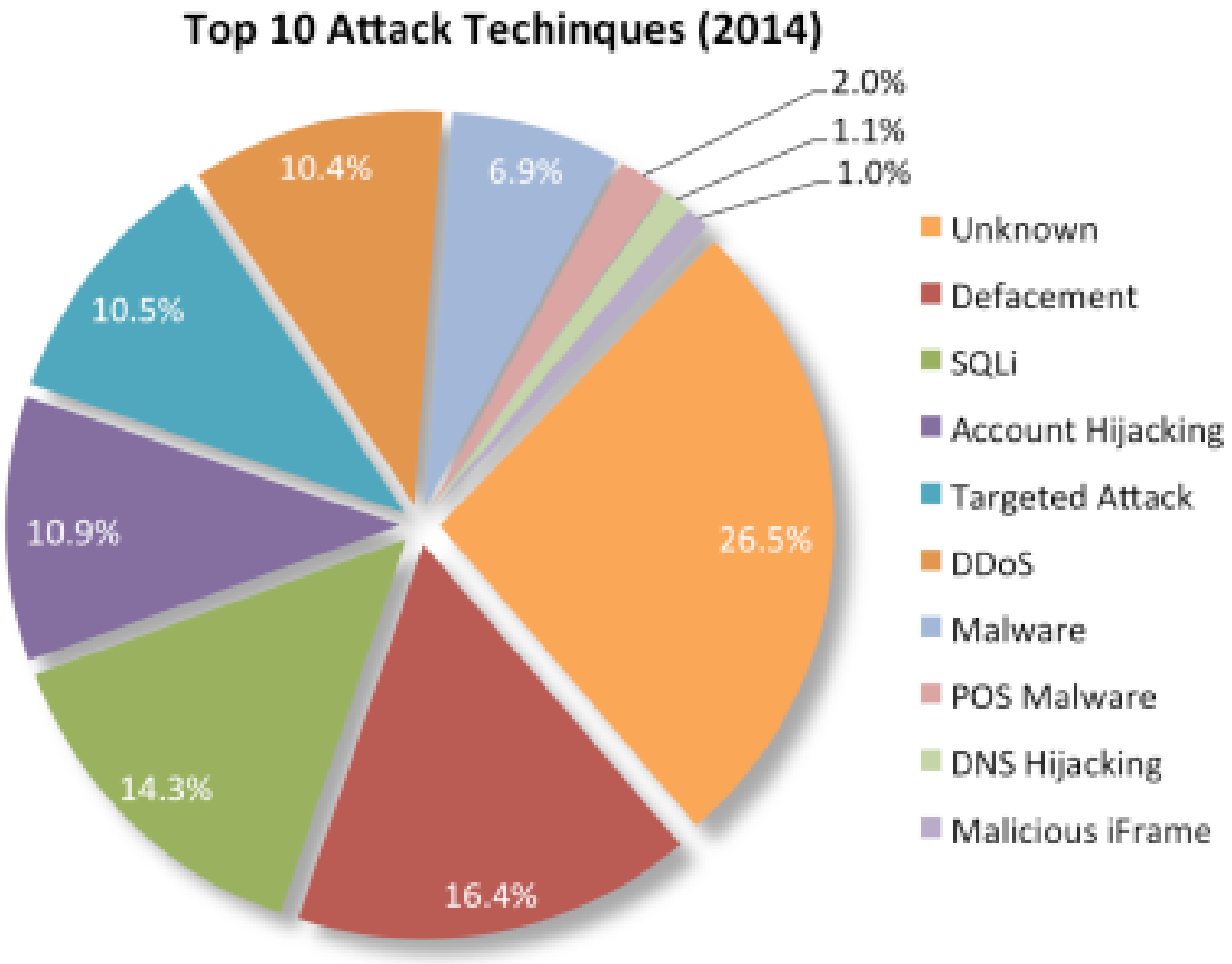
Intrusion & Anomaly Detection

Security Overview

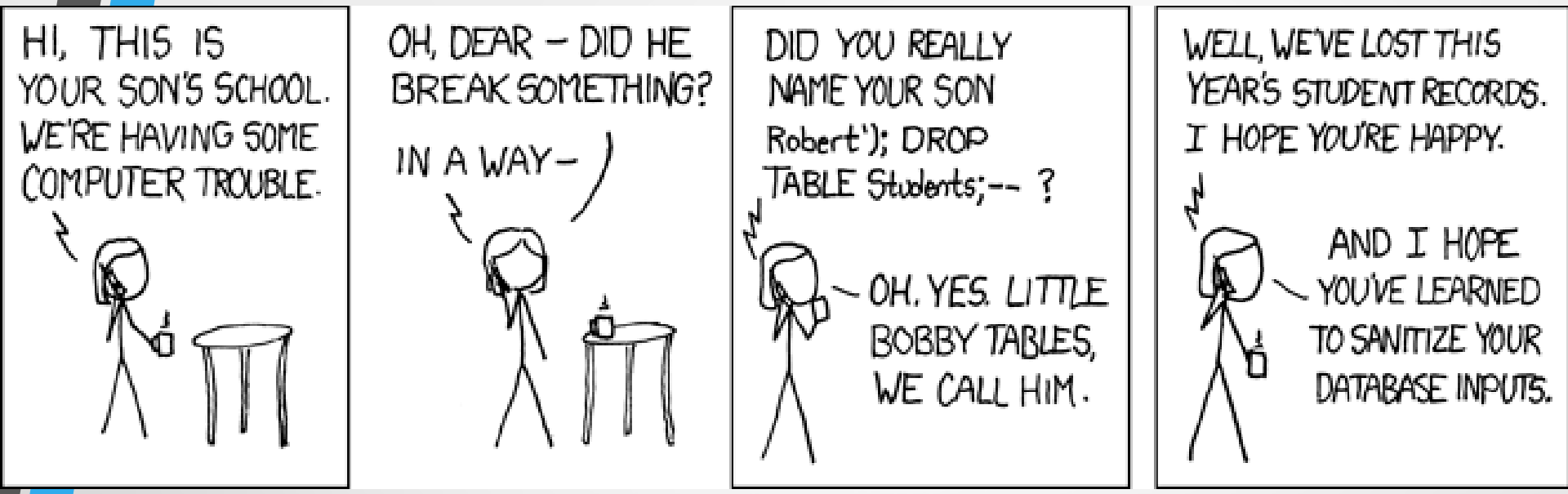
Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University



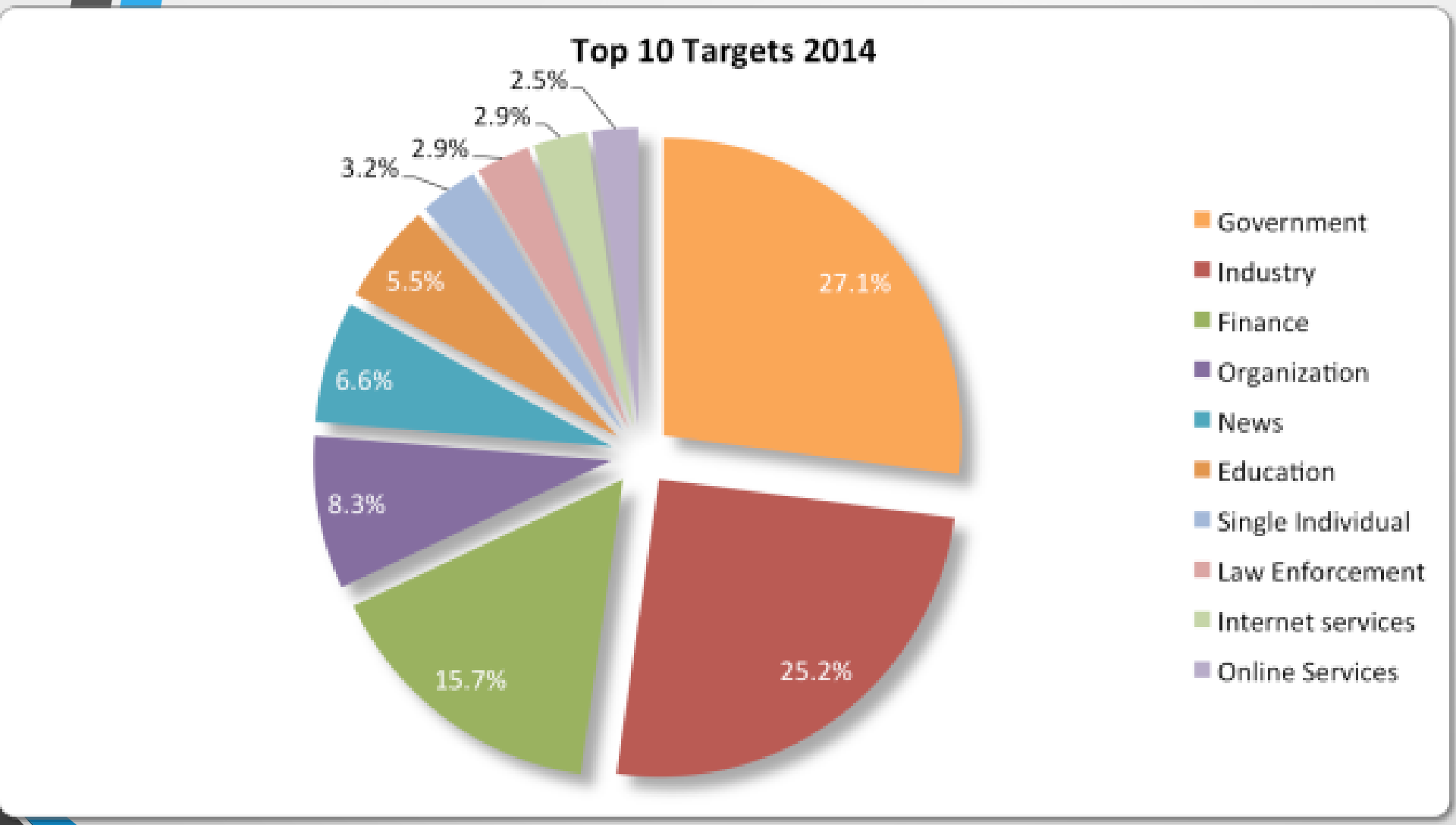
http://hackmageddon.com



http://hackmageddon.com



http://xkcd.com/327



http://hackmageddon.com

Terminology

- Threat
- Threat agent
- Vulnerability
- Exploit
- Attack
- Attack Surface

Security Services

- Integrity
- Confidentiality
- Availability
- Authentication
- Non-repudiation

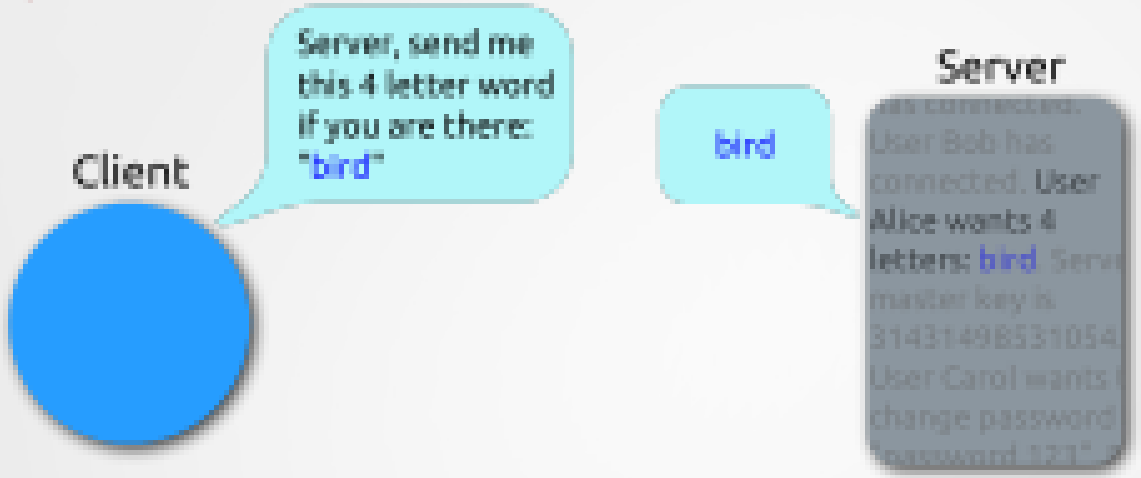
Level of Impact

- Low
- Moderate
- High

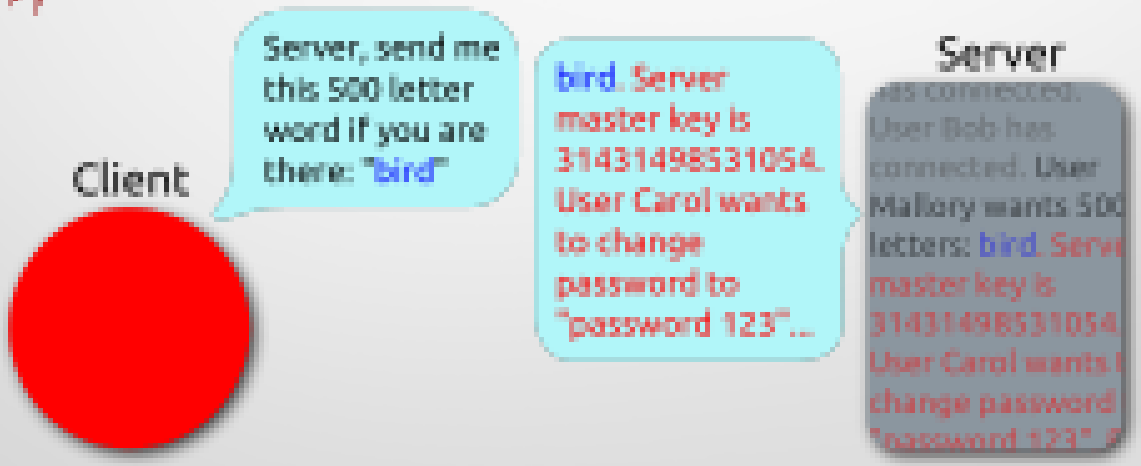
Types of Attacks

- Passive vs. Attive
- Denial of Service
- Reconnaissance
- Access
- Worms, Viruses, Trojan horses

Heartbeat – Normal usage

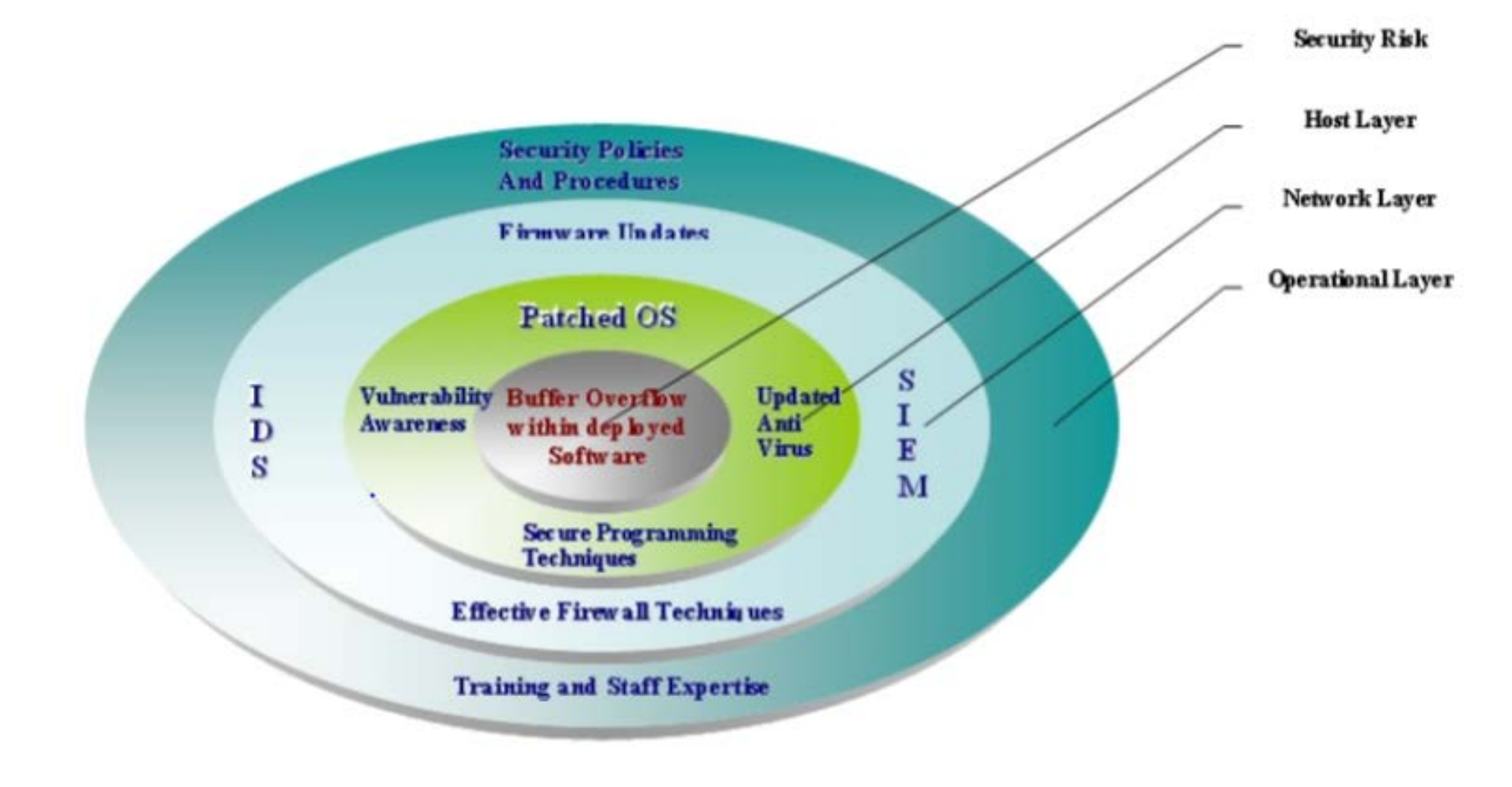


Heartbeat – Malicious usage



http://xkcd.com/1354

Network Defense in Depth



From: https://www.google.com/search?q=network+defense+depth&ie=utf-8&oe=utf-8

Router Compromise

- What can an attacker do if router is compromised?
- Possible vulnerabilities in a Cisco router configuration