



INTERNET SECURITY & FRAUD

Michael Richmond, CCNA, MCP, CISSP
Chief Operating Officer, P&N Tech
a division of Postlethwaite & Netterville

Essentials of Information Technology

Where we came from...

Where we are going...


Primarily single source
Largely asynchronous

Inside my organization

Static and pre-defined networks

You find information, people

Inside the firewall, walled off



Information

People

Communities

Context

Security


Multiple sources, multiple devices, multiple applications
Non real-time and real time, interactive

Dispersed teams, outside my organization

Dynamic teams

Right time, right people, right resource

Inclusive, selective, fluid



Current Threat Landscape



Top Security Threats

1. Workplace Violence
2. Business Interruption/Disaster Recovery
3. Terrorism (Global and Domestic)
4. Internet/Intranet Security
5. Employee Selection/Screening Concerns
6. Fraud/White-Collar Crime
7. Unethical Business Conduct
8. General Employee Theft
9. Property Crime (external theft/vandalism)
10. Drugs/Alcohol in the Workplace

Top IT Security Concerns

1. Securing remote access
2. Keeping virus definitions and AV software up to date
3. Patching systems
4. Monitoring intrusions
5. Securing file transfers
6. Network use monitoring
7. User policy awareness and training
8. Password management and administrative access
9. User training
10. Monitoring of system logs

Mobile Device Impact

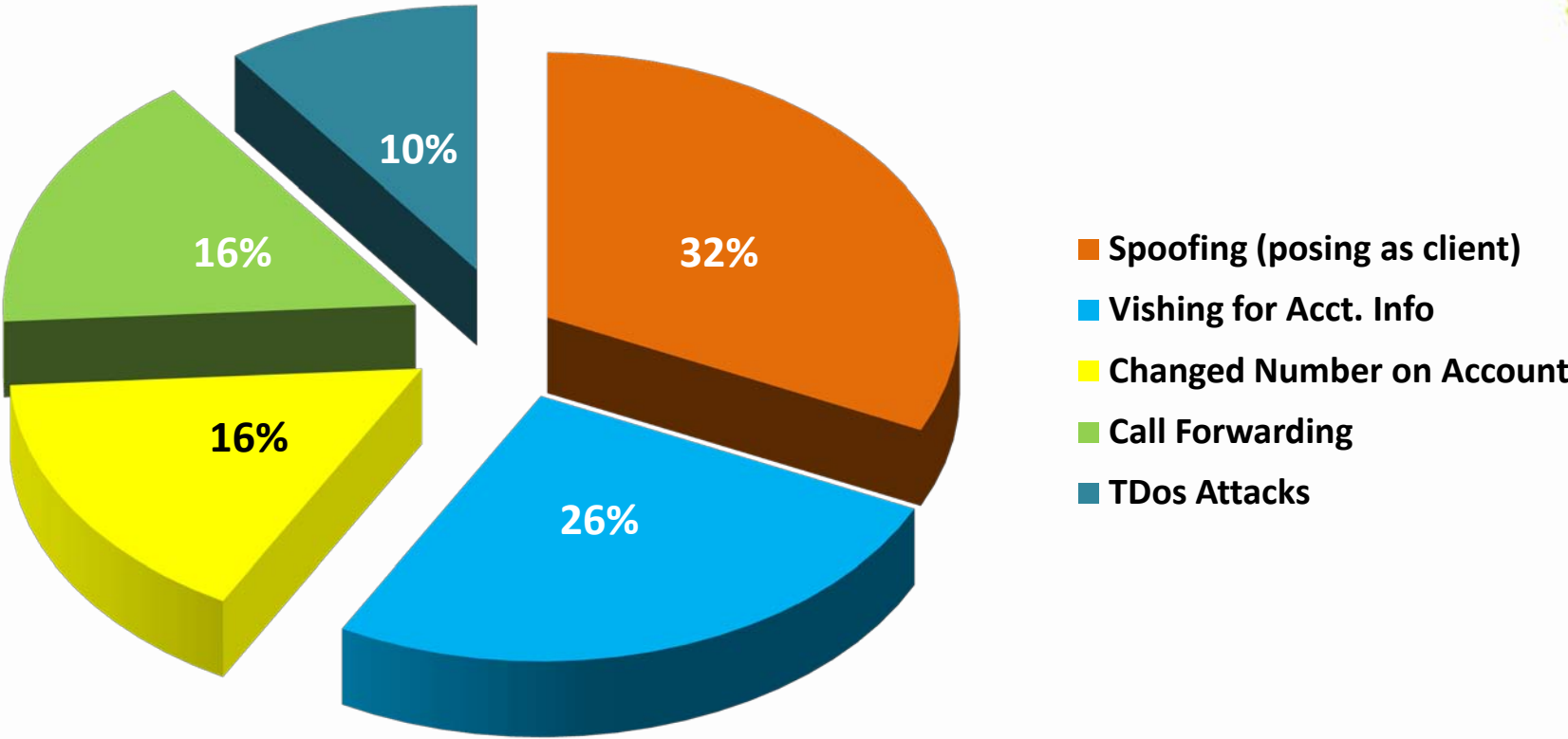


Hackers are increasingly targeting vulnerabilities in mobile devices – specifically the iPhone and the iPad.



CyFin MobileTrends: January 2011- Present

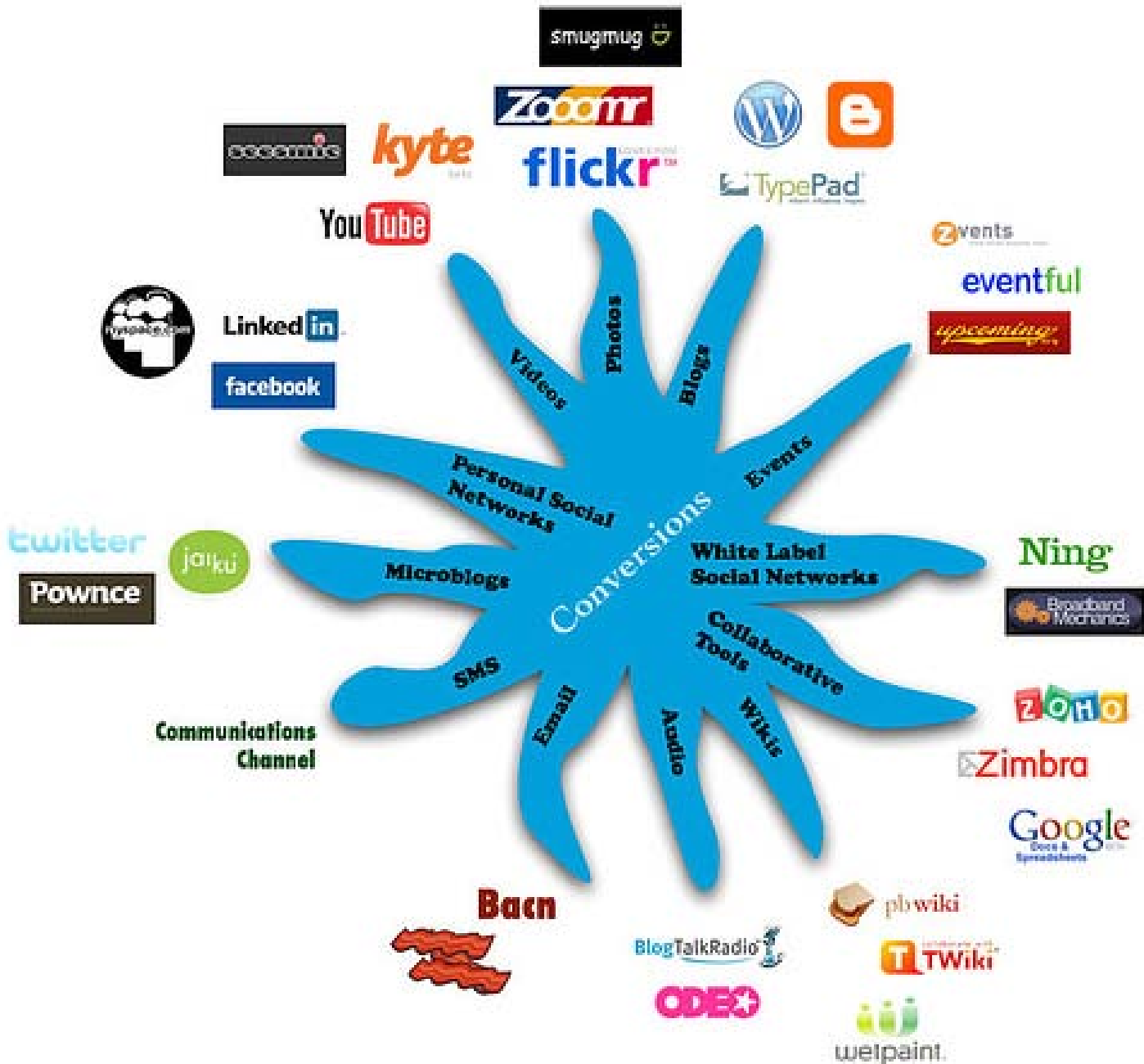
CyFin Listserv



Key Mobile Threats & Risks

Overlap to Tablets/Smartphones

Mobile Threat	Examples	User Risk
Misbehaving Apps	<ul style="list-style-type: none">• Network Abuse• Battery Drain• Memory Hog• CPU Spike	MEDIUM
Device Loss or Theft	<ul style="list-style-type: none">• Device Theft• Unauthorized Access	HIGH
Phishing/ Spoofing/ Web Scams	<ul style="list-style-type: none">• Online Banking Spoofing• Email/Web Phishing• Voice/SMS Phishing• Malware Download	HIGH
Network Attacks	<ul style="list-style-type: none">• Online Compromise• BOT Networks/DOS• Man-in-the-Middle Attack	LOW
Malware	<ul style="list-style-type: none">• Viruses• Spyware/Snoopware• Trojan Horses/Worms	MEDIUM





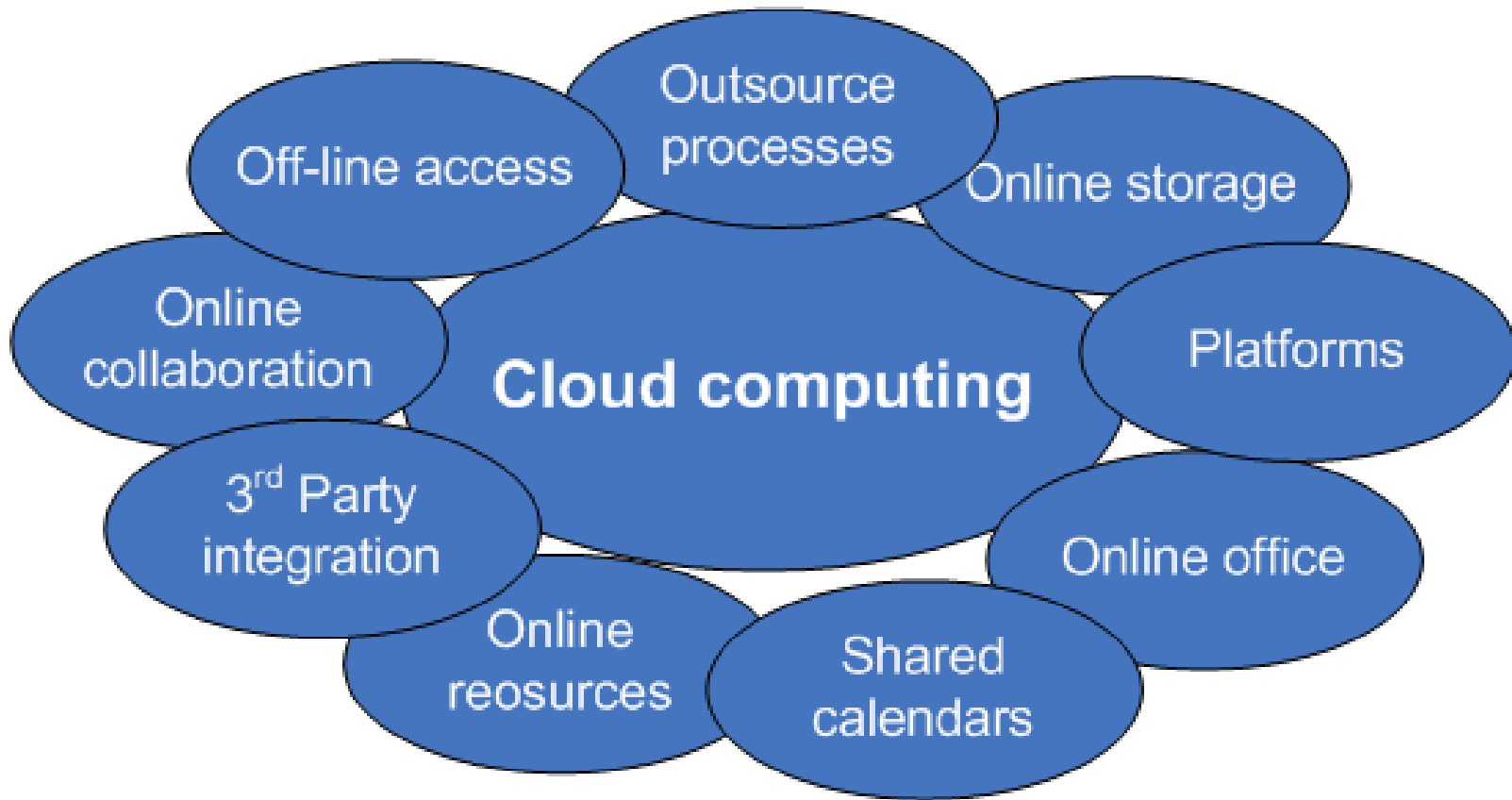
WikiLeaks



**To the
CLOUD...**



So what is the Cloud, exactly?



More scrutiny for “Cloud” security

- Popularity in Cloud services will continue to increase.
- Auditors will need to see a clear audit trail of application activity from end-users.
- Require tighter integration between Cloud applications and internal monitoring and security technologies and policies.

Risk vs. Reward

...not just for the
good guys.



Data breaches at schools and hospitals yield record-breaking financial losses in 2011.

- According to the Identity Theft Resource Center, educational and medical institutions accounted for more than a third of all data breaches in 2010, as well as some of the largest breaches of the year, including two at the University of Hawaii (nearly 100,000 records exposed), and AvMed Health Plans (1.2 million records breached).
- Ponemon Institute study concluding that data breaches were costing the healthcare field more than \$6 billion per year.

Security Real World Example



The Criminal Element



Building Blocks of an Exploit



Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.



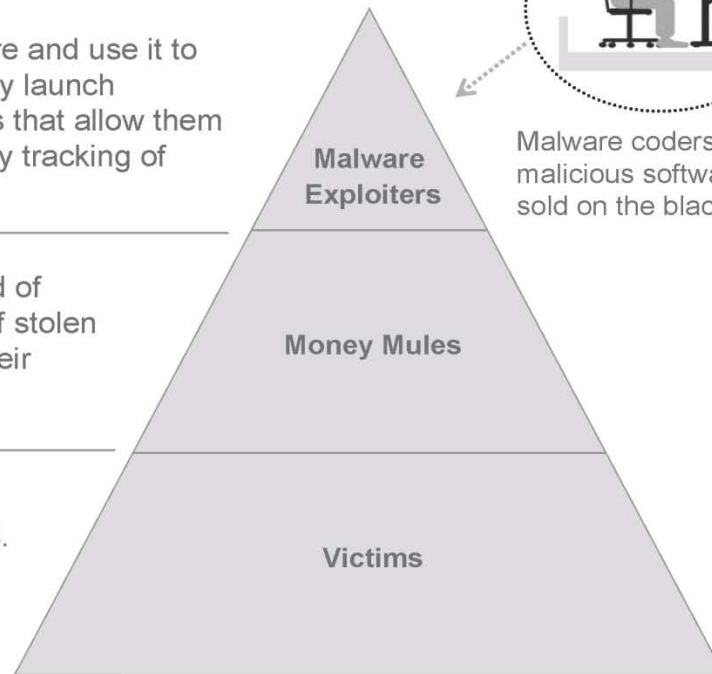
Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.



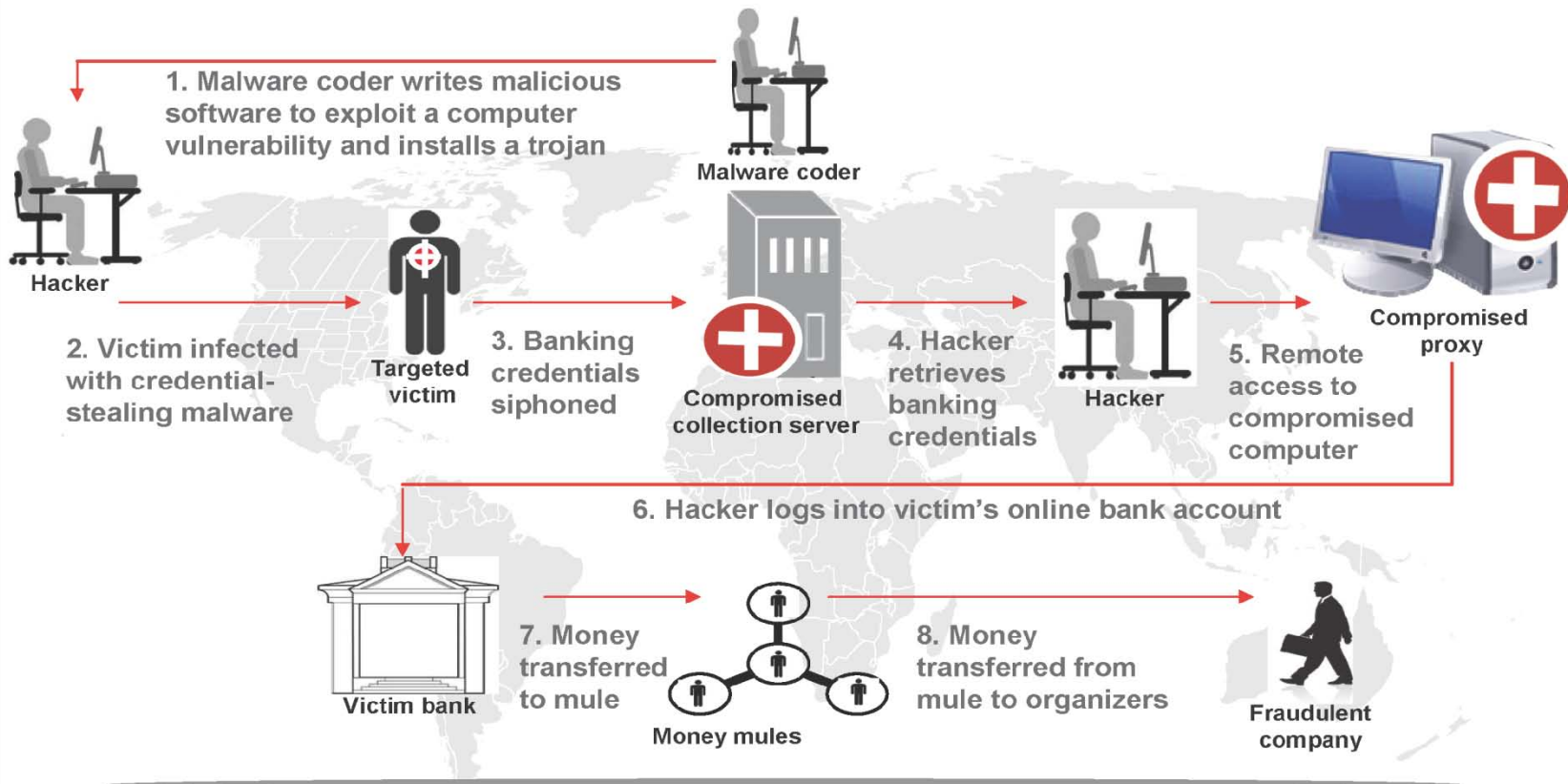
Victims include individuals, businesses, and financial institutions.



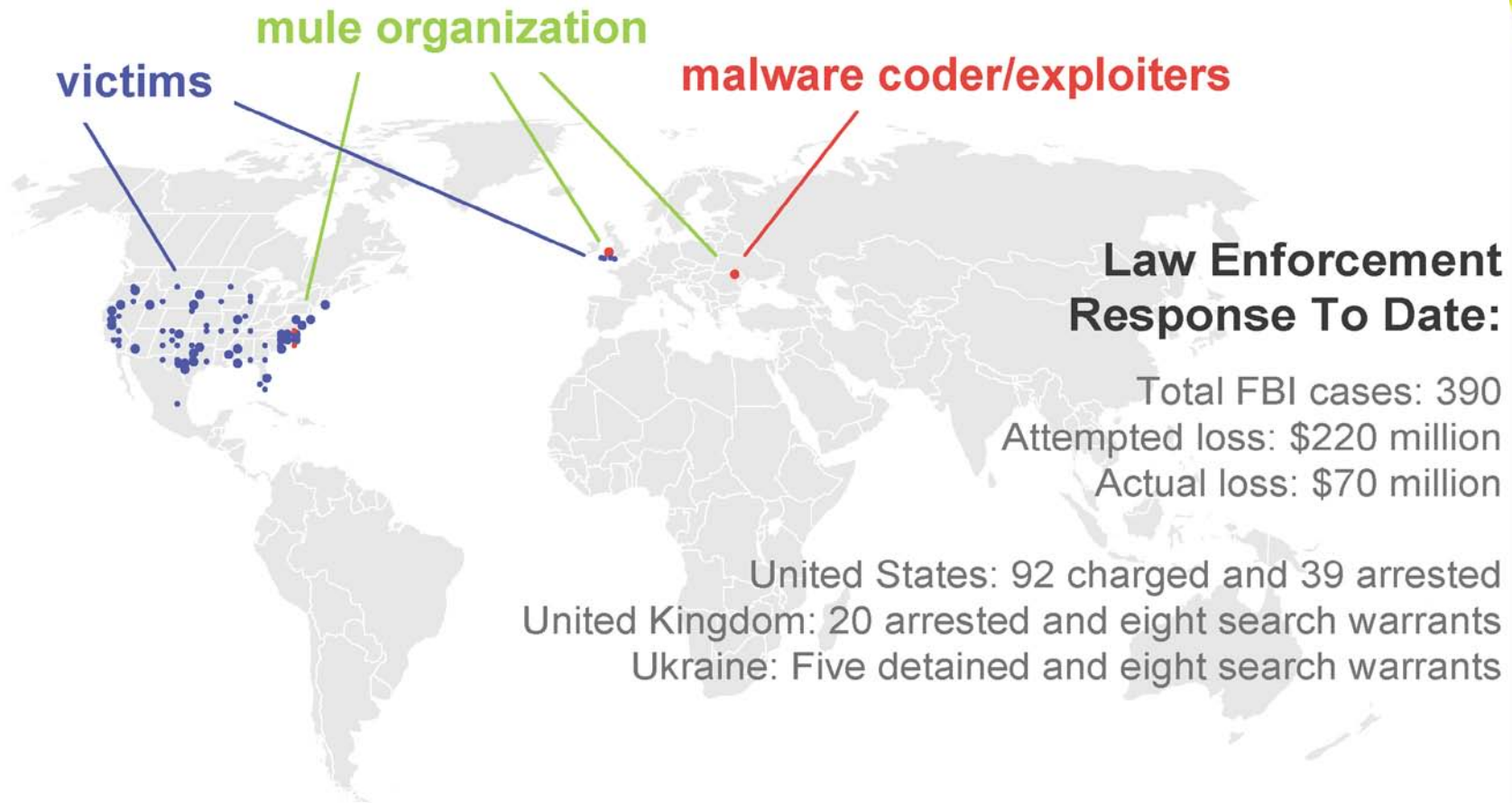
Malware coders develop malicious software that is sold on the black market.



Fraud- The Execution



Global Reach



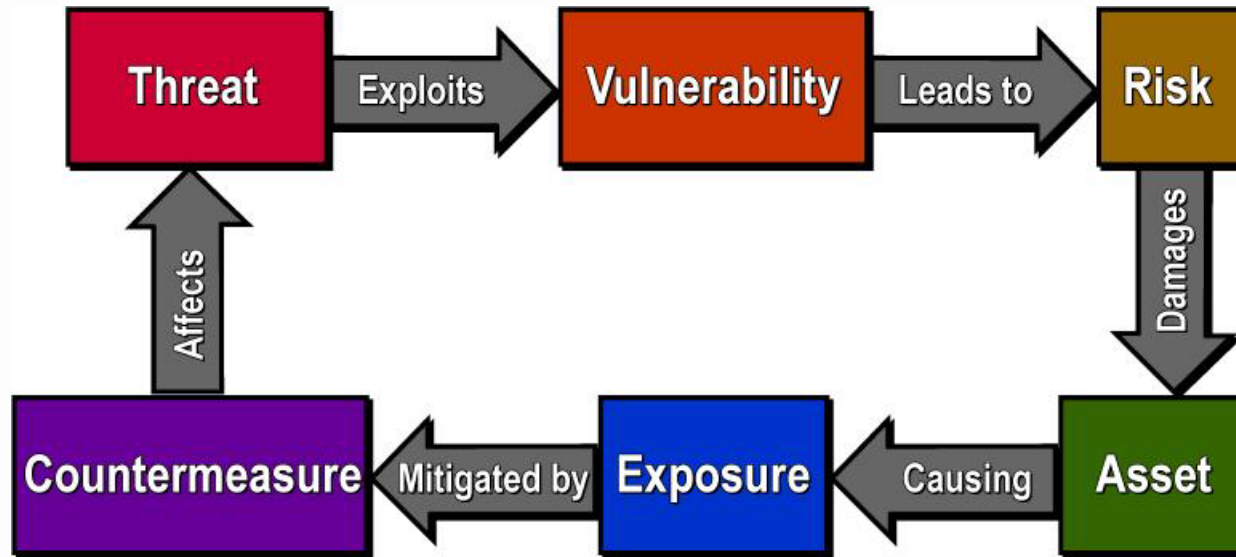
Reducing Risk in IT



RECAP-Top IT Security Concerns

1. Securing remote access
2. Keeping definitions and software up to date
3. Patching
4. Monitoring
5. Securing file transfer
6. Network use policy
7. User policy enforcement
8. Password management and administrative access
9. User authentication
10. Monitoring system logs

Risk/Countermeasure Relationship



Questions?