Cyber Security for Law Firms

Presented to the Louisville Bar Association

Justin Hall
Director, Security Services

CBTS

/usr/bin/whoami

Twelve years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Penetration Tester, Incident Handler, Forensic Analyst

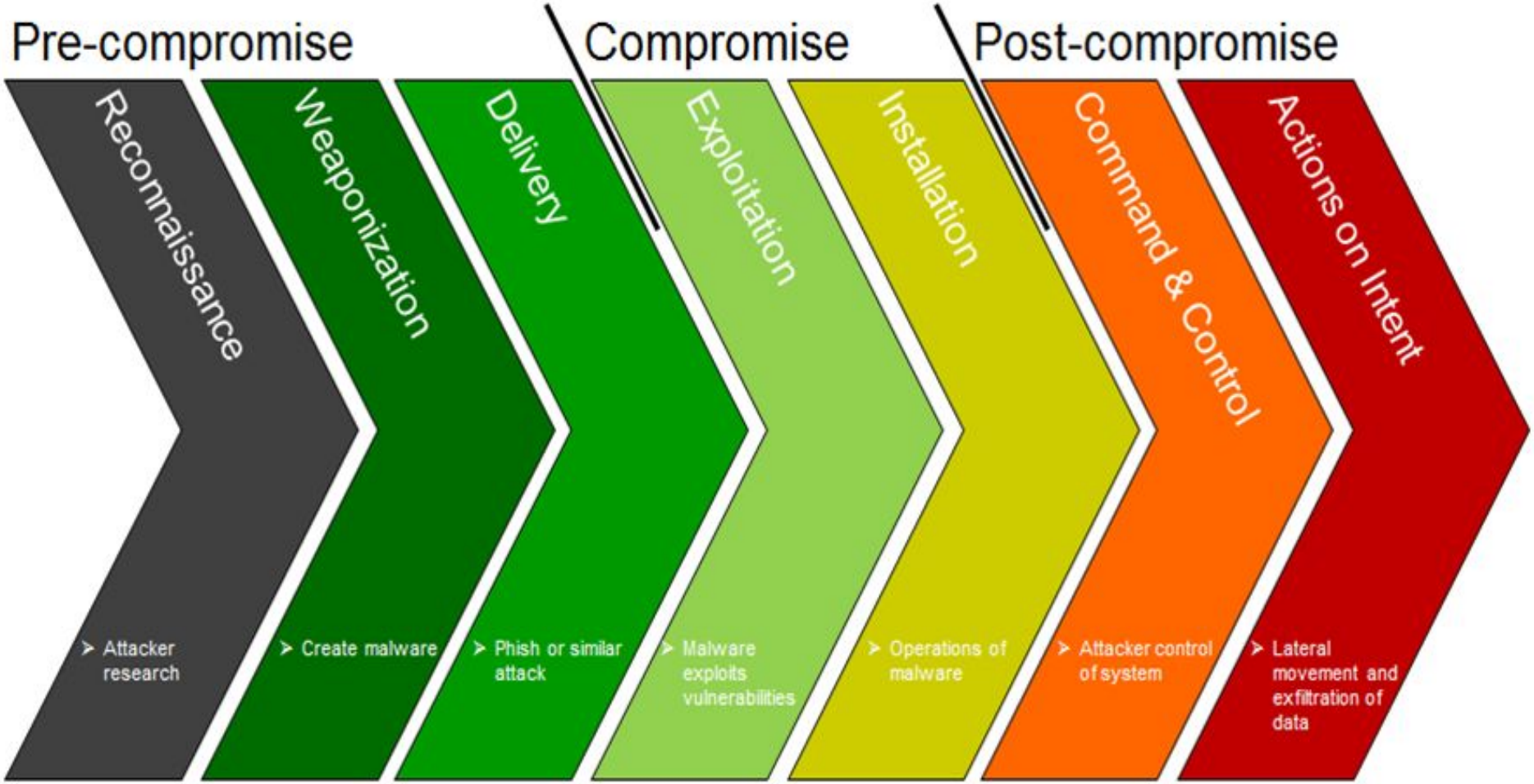
BSidesCincinnati cofounder

$81b

Gartner Says Worldwide Infosec Spend in 2016 Will Top $81.6 billion

http://www.gartner.com/newsroom/id/3404817

Who's attacking?
What do they want?
How do they **do it**?
How do we **stop them**?



The Cyber Kill Chain - Lockheed Martin, 2011

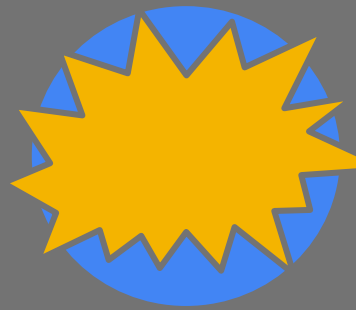
What are they after?

Bandwidth

Access

Sensitive Data

Money



Destruction

How do they attack?

Phishing
& Social
Engineering

Web App
Attacks

Exploiting
Listening Services

Password
Attacks

Local Attacks

Threat Models:

Who's attacking?
What do they want?
How do they **do it**?

Cybercriminals

Targets

Bandwidth

Money

Attack Vectors

Phishing
& Social
Engineering

Password
Attacks

State Sponsored

Targets

Sensitive Data

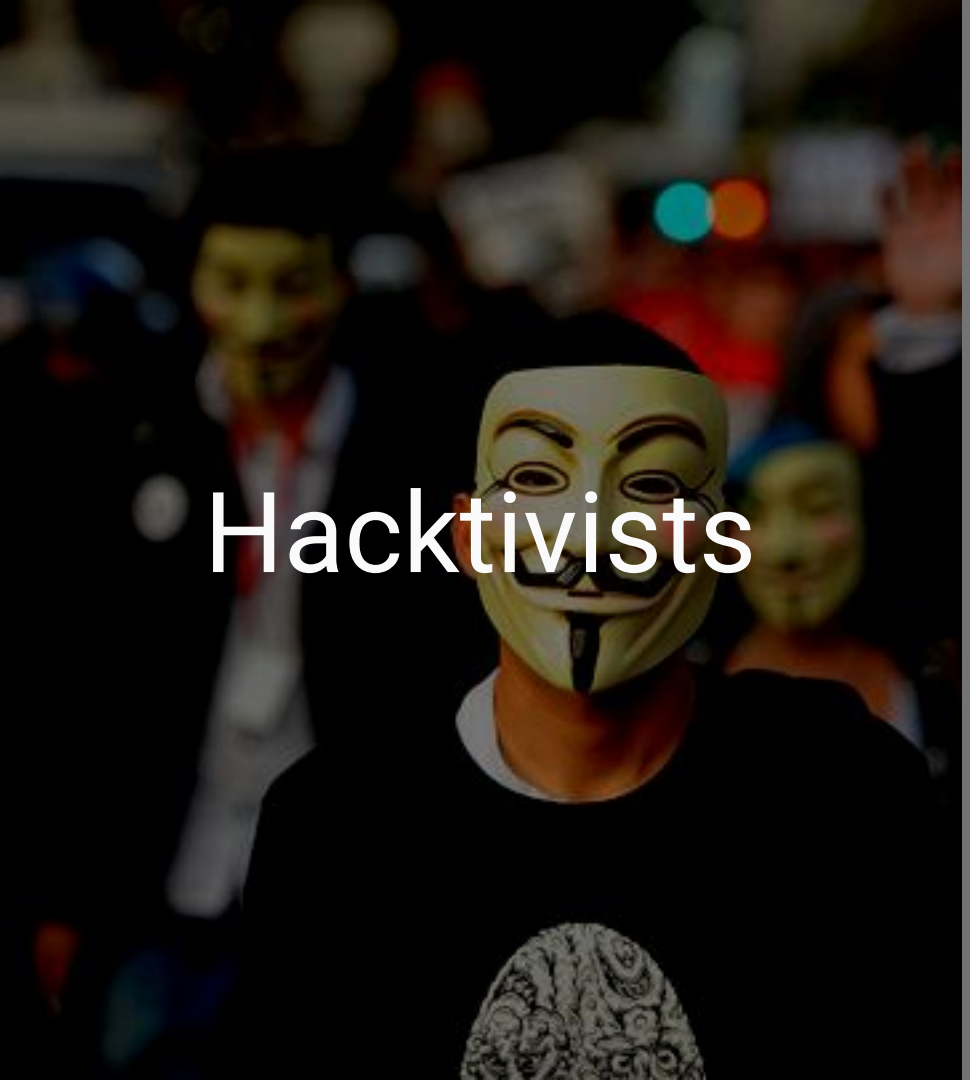
Access

Attack Vectors

Phishing
& Social
Engineering

Password
Attacks

Exploiting
Listening Services



Hacktivists

Targets

Bandwidth

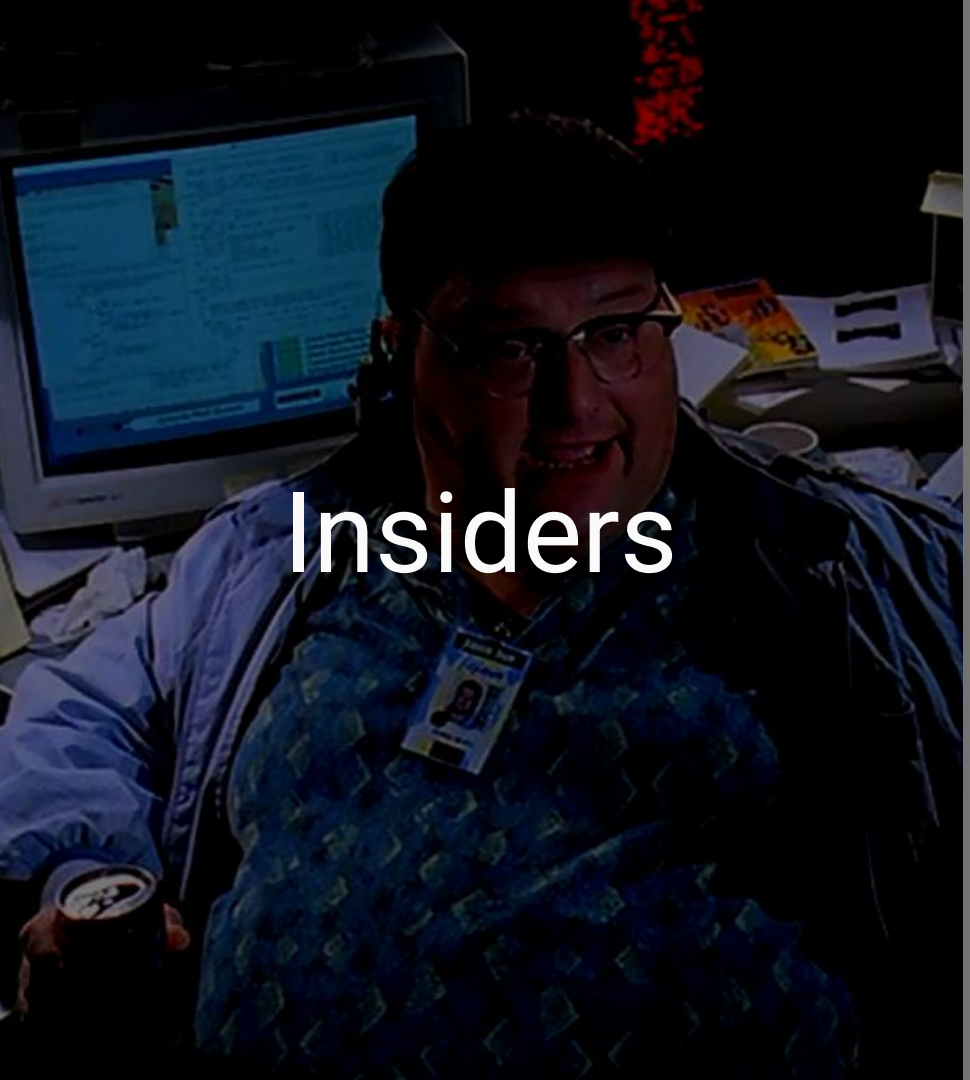
Destruction

Attack Vectors

Phishing & Social Engineering

Password Attacks

Web App Attacks



Insiders

Targets

Sensitive Data

Access

Destruction

Attack Vectors

Local Attacks

Password Attacks

Exploiting Listening Services

Mis-users

Targets

Sensitive Data

Access

Bandwidth

Attack Vectors

Local Attacks

Password Attacks

Top Security Controls:

How do we **stop them**?

Center for Internet Security®

The CIS Critical Security Controls for Effective Cyber Defense

1. Perimeter Defense

Content-Filtering Web Proxy

Sandboxing

Network IDS/IPS

Application Firewall

Layer 2-3 Firewall

SCAP-Based Filtering

2. Vulnerability Management

Patch Management

Vulnerability Assessment

Penetration Testing

Auditing

3. Secure Data Storage

Encryption

Data Loss Prevention

Multifactor Authentication

UBA

4. Monitoring & Response

Log Collection

Log Correlation & SIEM

Security Operations Center

Managed Security Services

5. Awareness Training

Phishing Simulations

Personalized Material

Formal Policies & Procedures

Up-To-Date

Q&A

@justinhall
justin.hall@cbts.net