RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Cyber Vigilante or Self Defense?

SESSION ID: STU-M06A

Bruce J. Heiman

Partner
K&L Gates LLP

THE PROBLEM

- Number and severity of cyber-attacks dramatically increasing
- Two kinds of companies
  - Those that have been hacked
  - Those that have been hacked but don’t know it yet
- Great imbalance between attackers and defenders
  - “The attacker just has be right once;

    the defender has to be right all of the time”

TRADITIONAL RESPONSES

- Prevention – keep the malware out
  - Firewalls; anti-virus software; encryption
- Mitigation – try to limit the damage
  - Shut the system down; pigeon hole
- Collaboration – call for law enforcement (and intelligence?)help
  - Do forensics on your system

ENHANCEMENTS CURRENTLY BEING CONSIDERED IN WASHINGTON

- Influence companies to deploy more defense
  - Offer liability protections or insurance incentives
- Improve information sharing between industry and government
  - Both ways
- Increase law enforcement resources
  - Manpower, training, cooperation

BUT IT IS ENOUGH?

- Can’t win (or survive/thrive) only playing defense
  - Need to change the attacker’s calculus
- The government will <u>never</u> have enough resources to protect/help enough private companies
  - Consider current numbers
- Should companies be able to respond?
  - “Active defense” – “Hack Back”

THE RANGE OF ATTACKING BACK – A FISTFUL OF ACTIONS

TRACK

HACK

SACK

JACK

WHACK

TRACK – ATTRIBUTION

- First Step
  - Whodunit and how?
- Essential
  - Danger of implicating innocent third parties
- Requires leaving your own system/network
  - Need to search and identify
- Techniques
  - Watermarking
  - Beaconing

HACK – INFILTRATION

- Access an attacker’s computer
  - Exploit flaws in attacker’s RATs
- Introduce code
- Gather intelligence about the attacker, methods, targets
  - What is on the attacker’s computers?
  - Collect content of files
  - Keystrokes, screen shots, picture of user

SACK – DELETION

- Once access has been gained to attacker’s computer
- Search for defender’s files
  - It’s defender’s stolen property
- Take action to prevent use of defender’s information
  - Delete
  - Encrypt
- Expose/warn of attacker
- Do not interfere with or harm attacker’s computer or network

(CYBER) JACK – EXPLOITATION

- Gain access to attacker’s computer/network and assert control
- Prevent further damage to defender’s computers/network
- Actively “spy” on attacker’s actions
- Create confusion
  - Deception and misdirection
- Contain attacks
  - Sink holing

WHACK – DESTRUCTION

- Once in control of attacker’s computers/network
- Disable attacker’s ability to launch new attacks
  - Malware to prevent functioning of computer
- Destroy information obtained from third parties
  - Wipe hard drive
- Direct changes to innocent third party computers (zombies) to prevent their use in future attacks
- Damage other “assets” of the attacker

THE RANGE OF ATTACKING BACK – A FISTFUL OF ACTIONS

TRACK

HACK

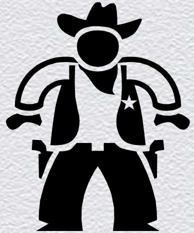
SACK

JACK

WHACK

BUT IT IS LEGAL?

- Concern about digilantism (digital vigilantes)
- DOJ CCIPS – says maybe not
- Federal Law: Computer Fraud & Abuse Act (CFAA)
  - Prohibits “unauthorized” access
- State Law: California Comprehensive Computer Data Access and Fraud Act
  - Prohibits access “without permission”
- International Law: Council of Europe Cybercrime Convention
  - Prohibits intentional access “without right”



U.S. COMPUTER FRAUD & ABUSE ACT

18 USC § 1030 (a) prohibits

- intentionally accessing a computer without authorization and obtaining “information from any protected computer” defined as a computer “used in or affecting interstate or foreign commerce or communication”

- knowingly causing the transmission of a program, information, code or command and as a result intentionally causing damage without authorization to a protected computer

CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT

- Section 502 Penal Code intent is to prevent unauthorized access to lawfully created computer data and computer systems
- Prohibits knowingly accessing and without permission

-- altering, damaging, deleting, destroying, or otherwise using any data, computer, computer system to … wrongfully control or obtain money, property or data

-- take, copy, make use of any data

-- use or caused to be used computer services

-- disrupt

-- access

-- introduce computer contaminant

COUNCIL OF EUROPE CYBERCRIME CONVENTION

- Directs each party to adopt legislative and other measures prohibiting the intentional commission, without right, inter alia:
  - access
  - interception
  - interference
  - misuse
  - forgery
  - fraud
- Establishes principles and procedures for international cooperation

POSSIBLE LEGAL RATIONALES FOR "SELF-HELP" ACTIVE DEFENSE

- It is permissible to employ reasonable and proportionate "force" to prevent …
  - Commission
  - Continuance
  - Completion

  of crime
- Possible rationales include
  - Self defense
  - Hot pursuit/recovery of stolen property
  - Citizen arrest of fleeing perpetrator (preventing escape)
- Key: when do actions = a new crime?
  - Case by case analysis can lead to uncertainty

BUT EVEN IF LEGALITY IS UNCERTAIN SO IS LIKELIHOOD OF PROSECUTION

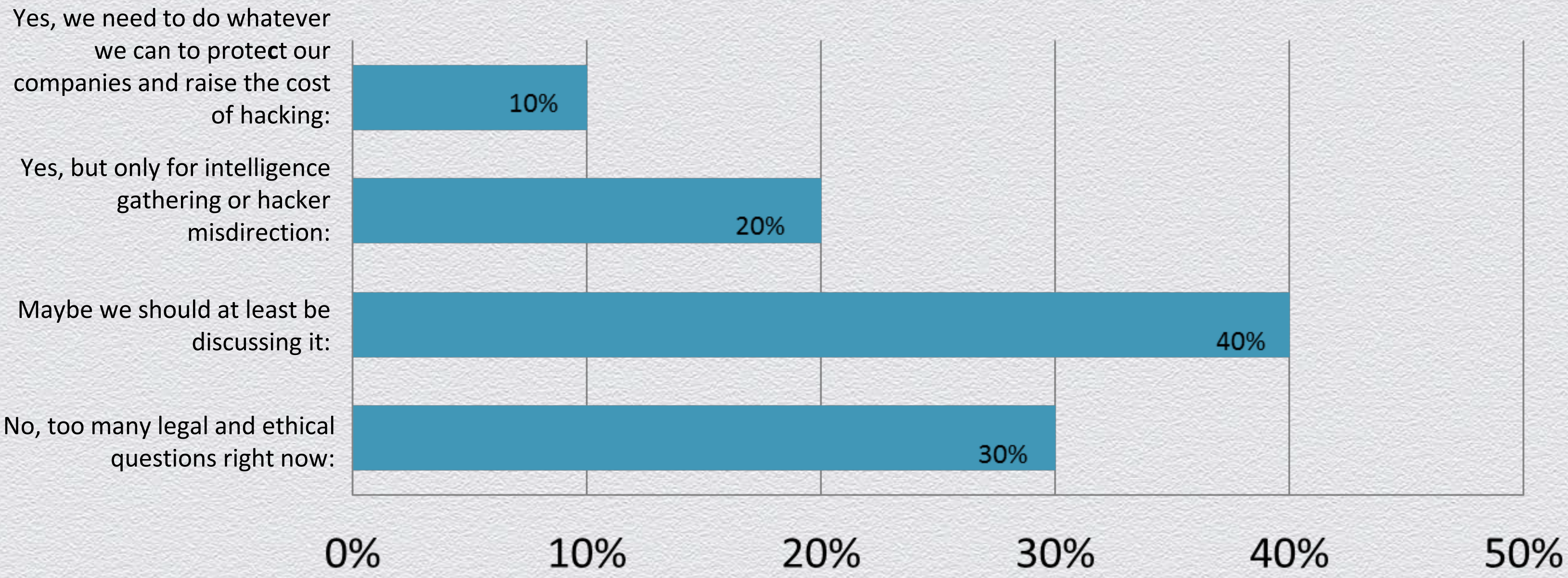
- ❑ The laws are clearly intended to stop the ‘bad guys’ and protect the innocent
- ❑ Will a prosecutor really want to pursue the initial victim?
- ❑ To make what point?
- ❑ And civil suit unlikely

BUT EVEN IF LEGAL OR WON'T BE PROSECUTED, IS IT WISE?

- ❑ Significant potential downsides
- ❑ Misattribution
- ❑ Retaliation
- ❑ Retribution
- ❑ Escalation

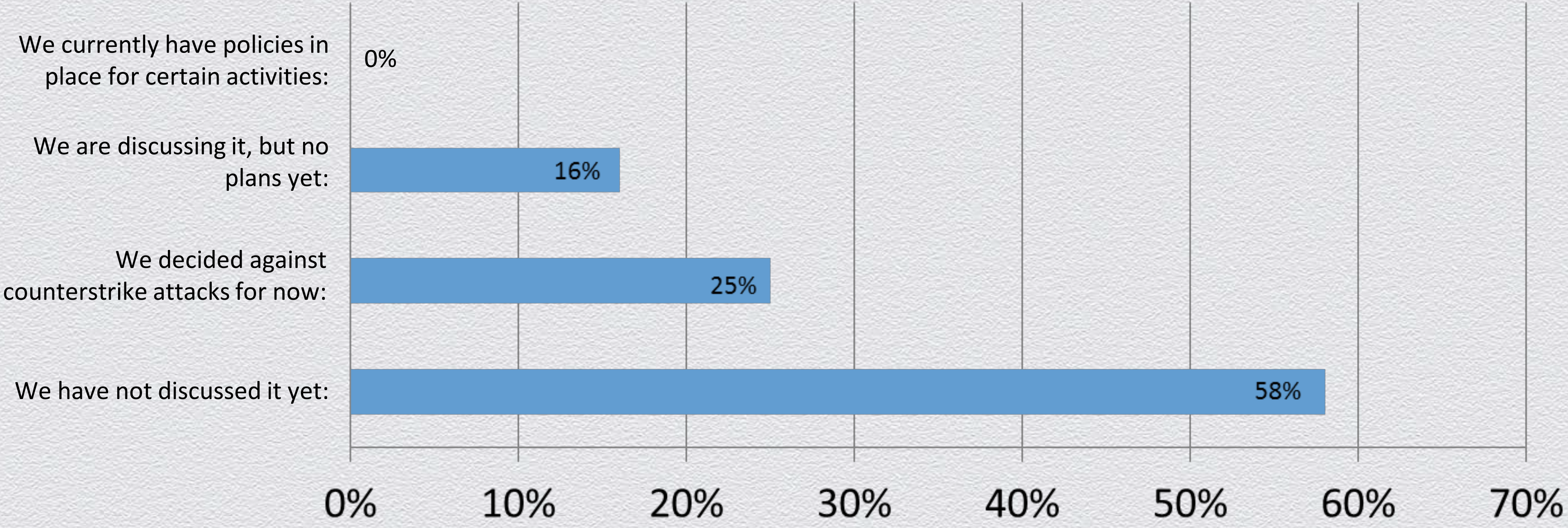
WHAT ARE COMPANIES THINKING? (Wisegate, April 2013)

Many in the industry think it’s time to start counter attacking the hackers, as the best way to limit their damage and start stemming the tide. What do you think?



WHAT ARE COMPANIES THINKING? (Wisegate, April 2013)

Has your company developed counterstrike policies to deal with cyber attacks?



K&L GATES

#RSAC

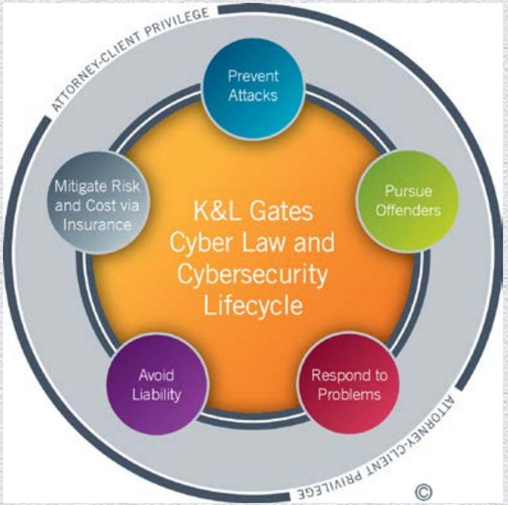
RSACONFERENCE2014

IN SHORT –
COMPANIES ARE BELLYING UP TO THE BAR—
IS IT TIME TO ORDER A DRINK?

K&L GATES

QUESTIONS?

- Bruce.heiman@klgates.com
- 202-661-3935


ATTORNEY-CLIENT PRIVILEGE
Prevent Attacks
Pursue Offenders
Respond to Problems
Avoid Liability
Mitigate Risk and Cost via Insurance
K&L Gates Cyber Law and Cybersecurity Lifecycle
ATTORNEY-CLIENT PRIVILEGE
©

K&L GATES