An Abstraction Layer Between Information Security and Law Enforcement

Nick Selby

SecTor 2011, Toronto

19 October 2011
Let's Crime!

If you could commit a crime right now that would bring in lots of cash and present very little risk to you personally, what would you do?

Cyber Crime! FTW!
Who We Are

David Henderson

- Patrol sergeant, 15-year veteran @ DFW-area agency
- Warrants officer; USMS Fugitive Task Force member
- Investigator/detective
- Cyber-crime investigator, forensics, mobile forensics
- TCLEOSE Instructor

Nick Selby

- Sworn in 2010; Intel Analyst (Appointed in 2008). Patrol, Warrants @ DFW-area agency
- Data theft/industrial espionage consultant, since 2005 advised F500 corporations, governments
- Former VP, Operations/Founder and Director of Enterprise Security Practice, The 451 Group
- Former faculty, IANS
Caveats

- I do not speak on behalf of, or represent, any police agency.
- Opinions expressed here are my own. Information in this presentation is not legal advice. It is not advice at all.
- Everything I say here is for entertainment purposes only.
- My opinions do not necessarily reflect those of any law enforcement agency, administrator or police officer anywhere in the world.
Agenda

The Problem
How the problem manifests itself
Some ideas for solutions
Discussion
When Do You *Have To* Call The Fuzz?

CONSULT A LAWYER – AND I AM NOT ONE. USE AT YOUR OWN PERIL. THIS IS NOT POLICE ADVICE. I’M NOT ADVISING YOU. THIS LIST IS WORTHLESS. I’M NOT KIDDING.

Child Porn
- Three images or more

Financial Data
- More than US$100,000

Physical Plant
- Things that go ‘Boom’

Export Control
- Government restricted data
No one wants to call the po-po.

**Disrupt**
- Cops treat our network and our business like a crime scene
- If you can even get them there

**Growl**
- Cops are dense, suspicious and unfriendly

**Loud**
- I can handle this
- I don’t want the media – and I really – don’t want our customers to know we’ve been hacked
Why Not Call The Po-Po?

Because when you call them, they come. When they come, they tend to come \textit{en-masse}.
And sometimes? They get mad. God knows what they’ll do.
Except we all know they’ll do this

Every cop wants to walk in front of the cameras, badge on a lanyard, grim expression on his face.
But it’s not just the cops . . .

Enterprises organize security and networking in an ObamaCarean manner straight out of Kafka

Information security has all the responsibility and none of the authority to affect change...
Diametrically Opposed Roles

• Want to things to go with the flow
• Are judged by up-time

Network People
Diametrically Opposed Roles

- Want everybody to stay right where they are…
- Are judged by ... Hmmm…

Security People
Eventually . . .
"YEAH, HI. I’M CALLING ABOUT my company bank account in the Bank of New York/Mellon? It was bilked for $60K, which was sent to the Ukraine, after my servers in Georgia were compromised? After someone put malware on my terminals in Texas and got my credentials, and did an online transaction on the bank's website? Whose servers are in California."

Who you gonna call?
Some Things To Take On Faith:

- Cops want to help, they’re just really clueless about how to go about helping.
- They can’t quantify/articulate the damage to a prosecutor for you.
- “Tech-savvy” is not a prerequisite to join the force.
- They really understand the process of getting to a solution from a legal standpoint.
- They really don’t want to work the case, only to have it snatched from them by another agency.
There are very sharp people in the FBI.

The majority of the FBI's special agents are seriously dedicated to helping people and to solving crime.

Do not conflate “overworked” with “uncaring.”


(But let's talk about how FBI gets its funding....)
FBI FY 2011 Budget

On what metric do they rate success? The Uniform Crime Report for murder, rape, robbery, aggravated assault, burglary, larceny-theft, and auto theft.

Overall:
$8.3bn; 13,057 special agents, 3,165 analysts, 17,588 staff

Cyber:
163 new positions (63 SAs)
$43m in additional funding

0.021% increase and 0.55% increase, respectively
The Cop’s Perspective

You can't just tell a cop, “I GOT Pwnz0rd!”

It's all about money. DA's are elected. Judges are elected. Chiefs answer to the city council and mayors. Tell these guys what happened.

“My company's servers were breached as described in PC 33.02 and benefits were obtained and damage caused in excess of $62,000 (3rd degree felony). The attacks came from an IP address in Louisiana.”
A Case Study

- Scam: POS terminals get hit for $200 a pop, >$5m annually
- Call: CISO talks to LE, hears that, if he can show it's organized, help is on the way
- Quiz: Investigation; 80% of attacks emanate from IPs in US state of Georgia
- Drop: Provides feds with logs, evidence and explanation
- Pounce: Federal and state LE moves, makes arrests
- Bwe-YAW: Press releases, chest-bumps, Red Bull, new tactical trousers all around.
Why that worked

The target company was large enough to have contacts at local, county, state and federal law enforcement;

Those contacts understood the problem enough to tell target company what they needed to move ahead

Company could then focus its resources on providing what LE needed to move forward
The Problem

Most companies are not big enough to have these kinds of contacts.

Great organizations like InfraGuard and the like make a difference, but smaller companies don't participate enough.

Smaller-scale crimes affect businesses as well – skimmers, ACH/Wire fraud, stolen gift cards, organized shoplifting gangs, etc.

In relatively sophisticated “cybercrime,” law enforcement does not have the resources to help those who can't help themselves.
But wait!

“Relatively sophisticated cyber crime”? *Bullshit!* This is just theft.

Let's not get caught up in the hype: When we're hacked, people are breaking into our property to try to rob us. That is a business model dating back centuries. It's illegal. There are laws against it.

The only thing different is the type of window they're breaking, and the kind of silverware they're stealing.

What we need to do is give more businesses the ability to articulate the problems: here's what happened, here's what was stolen, here's how much it cost us to fix or replace.
What We Need

- Cross-trained / information security and law enforcement
- Local, state, federal Law Enforcement Officers who understand how to navigate the rocky shoals of case creation, prosecution
- ITSec people who have successfully prosecuted hackers, with LE connections
- Folks like you
- IT Professionals willing to take steps to protect the flock, to act as interpreter, to give of their time for the greater good
Imagine an Organization...

- It must be non-profit, provided at no cost
- It must be bi-lingual (IT/LE)
- It must comprise people trusted by either or both communities:
  - Both IT and LE communities operate on extended trust relationships
- All members must have widespread trust in the community, vouched-for
Proposal: CopCon@DefCon

Cops
- State, County, Local

InfoSec
- CISO, Analyst, Engineer, Forensics Guys, Threat researchers

Train Each Other
- 1 Day InfoSec to Cop
- 1 Day Cop to InfoSec
Sponsorship, User Support

- It can raise money to fund itself, sponsorships from vendors;
- Hold training sessions at conferences – sponsor money can pay to get cops there, because they have no budget. They’ll come.
- Maybe it's like a Linux User Group, volunteers with a common interest;
- It must interoperate with and establish standards, like an OWASP
- Its supervisory board will be cops, infosec guys, CISOs and malware/pen-test/reverse-engineering guys;
People Who Hate This Already

The FBI Guy From Central Casting: “Sounds risky.”

The InfraGuard-Is-The-OnlyGuard: “Why does anyone need this? Why, we've been doing this for years!”

The Cop From Central Casting: “Yeah? It's awful terrific we got someone as experienced as you ta come an' tell us how to investigate.”

The Ass-Covering Infosec Guy: “No really, I got it covered. We don't want our secrets in the hands of outsiders...what if they go to the media?”

The Vendor: “We do incident response for a living”
Talk To Me...

Where do we take this?
What's wrong with the concept?
What's right with the concept?
Which stakeholders did I leave out?
Who's In?

nick.selby [at] tridentrm.com
347-675-8295