Security Culture

Chicago
Cypherpunks Club

Freddy Martinez

Why?

Going to jail sucks

Keeps you or your people out of jail

We don't have the backing of security state

Opening question: The best way for an adversary to gain sensitive information?

Zeroth Rule

Zeroth Rule

Don't get caught

Threat Level: Midnight

Operation Model

What are we trying to do?

How are going to try to do it?

How do we *communicate?*

Considerations:

When do we switch it up?

How do we clean up?

Consequences of your actions

Compartmentalize

Idea: Separate information into *discrete* and *independent* cells

Critical: Don't Cross Contaminate

See also: Ross Ulbricht / a.k.a. DPR / a.k.a. fr0sty / a.k.a. altoid

Identity Management

Anonymity is *not* enough

Change identities and *unlink* them

Tactics Matter

Change them

- That's why they are *tactics*...

Never reveal your internal tactics (*how...*)

Never reveal your intended target(s) (w*ho, where, when...*)

The Wire: S03 E11

"Stinger's phone isn't on the same *network* as *everybody below him*."

"And Shamrock has a separate phone for calling [Stringer] Bell. We can't hear those calls because the system is *compartmentalized*"

Cell phones

Idea: Your phone will burn you

Cell phones

Idea: Your phone will burn you

Lesson: Use a burner

Cell phones

Idea: Your phone will burn you

Lesson: Use a burner

OpSec for telephony is very hard – you're doing it wrong

Critical: The dumber the phone, the smarter your security

Cell phones

“There's no pattern. Sometimes he calls every two weeks, sometime every three weeks. There's no consistency. I can't predict when he's going to make another call because the guy's erratic”

Zero Dark Thirty

STFU

Keep all information on a need to know basis

- Unless someone is sharing the risk (i.e. jail time) they don't need to know

Avon Barksdale: "Yo, y'all [redacted] talk too damn much man" (S01E11)

STFU (Pt 2)

Lesson: Listen to Avon

Security failures happen *all* the time

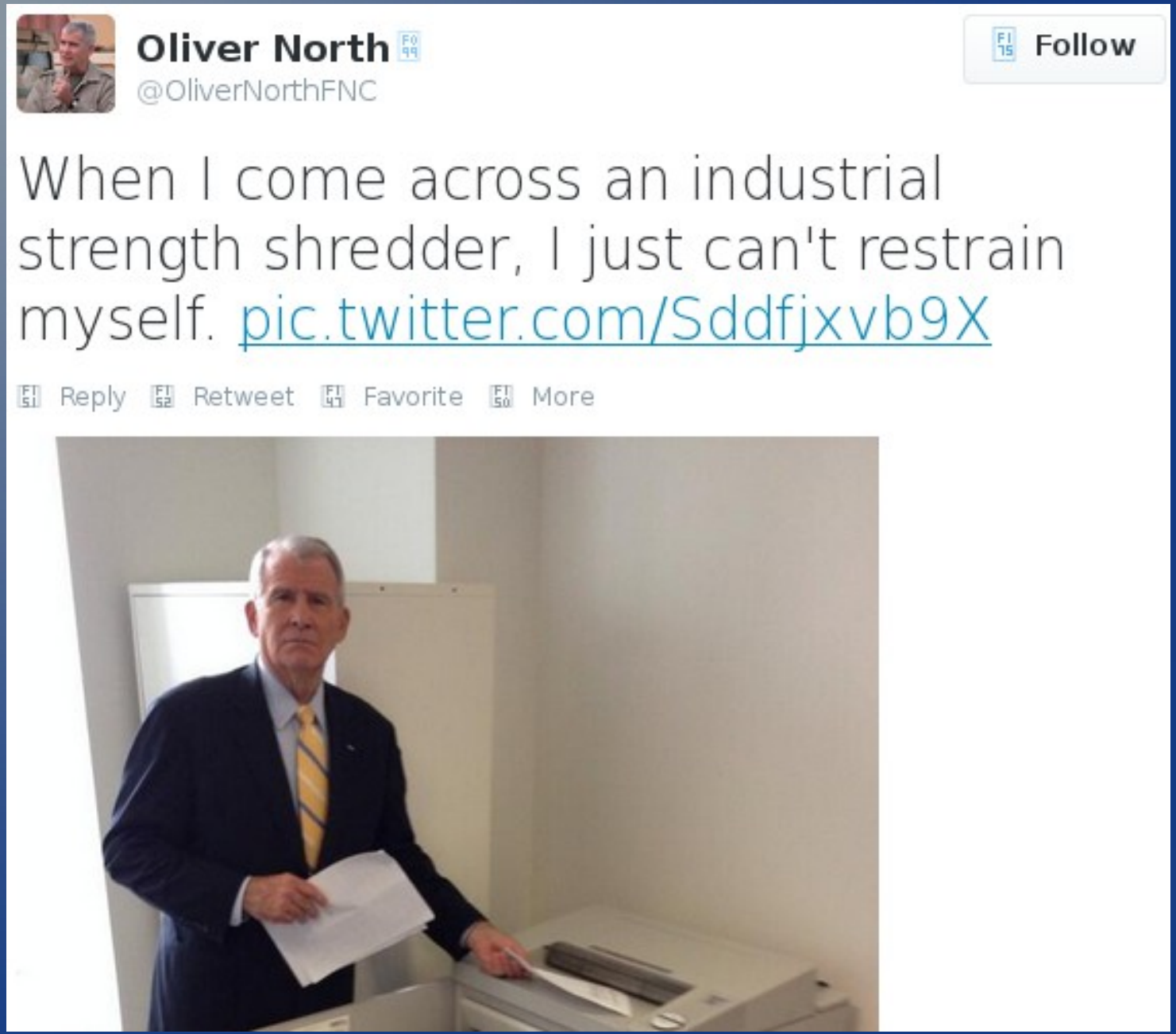
Critical: You (or one of your people) only have to mess up *once*

Logs

Idea: Don't Keep Them

Critical: No Logs, No Crime

LOL rite?


Oliver North
@OliverNorthFNC
Follow
When I come across an industrial strength shredder, I just can't restrain myself. pic.twitter.com/Sddfjxvb9X
Reply
Retweet
Favorite
More

Security Culture Cont.

Be cautious but not paranoid

Keep your personal life *personal*

Never talk to the police

- It's your lawyer's job to talk to the police
- It's your job to shut up

Final Thoughts

Fear leads to poor decision making

Trust your gut

You can't turn this shit on *retroactively*

Shut up

Links / Sources

Indymedia (Photos)

http://www.slideshare.net/grugq/opsec-for-hackers

http://grugq.github.io

“Rats! Your guide to protecting yourself against snitches, informers, informants, agents provocateurs, narcs, finks, and similar vermin” rats-nosnitch.com/rats/#ch3

Links / Sources

“Choosing Your Friends Wisely for Illegal Activities”

http://shawnewald.info/aia/sec_friends.html

The Back Door (Story about Hacker OpSec)

http://www.cjr.org/feature/the_back_door.php?page=all

Questions?

Image from flickr: Brian Lane Winfield Moore