Evertas

Cyber Security in US Non-Federal Law Enforcement

NATIONAL ACADEMIES *Sciences Engineering Medicine*

Committee on Cyber Hard Problems

Nick Selby, September 26, 2024

PUBLIC

About Me.

Blackhatonomics
Investigating Internet Crimes
In Context
Cyber Attack Survival Manual
Cyber Attack Survival Manual

Blackhatonomics: An Inside Look At The Economics of Cybercrime (Syngress 2012)
In Context: Understanding Police Killings of Unarmed Civilians (Contextual Press, 2016)
Cyber Attack Survival Manual (Weldon Owen, 2017, 2020)
Investigating Internet Crimes (Technical Editor) (Syngress, 2013)

I do **not** speak on behalf of any law enforcement agency. All comments given here are my personal opinions.

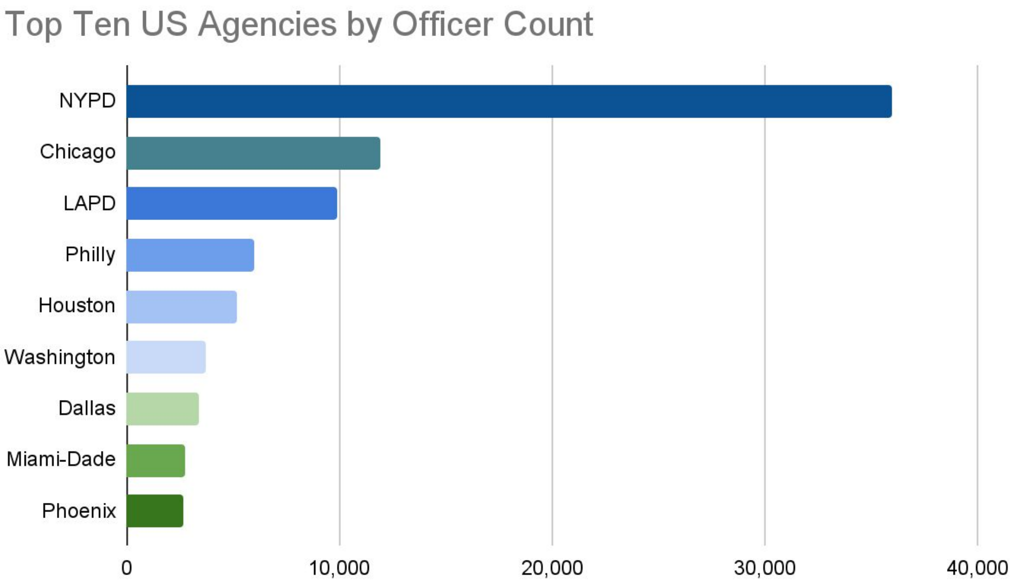
Co-host, with Chris Swan, of the Tech Debt Burndown podcast (2019-)
Co-host, with Peter Moskos, of the Quality Policing Podcast (2015-2018)

How It Should Be

- In my time at the NYPD, Yosef Lehrman was CISO, and did amazing things with defense-in-depth and great practices—including a level of network segmentation that can only be described as “diabolical.”
- In the time I was there, there were probably 10 or 12 incidents and I don't know of any that affected more than seven machines. Usually it was three or four.
- That’s great!
- But the NYPD is to American Policing as New York City is to America. Let’s see what that actually means.

Evertas

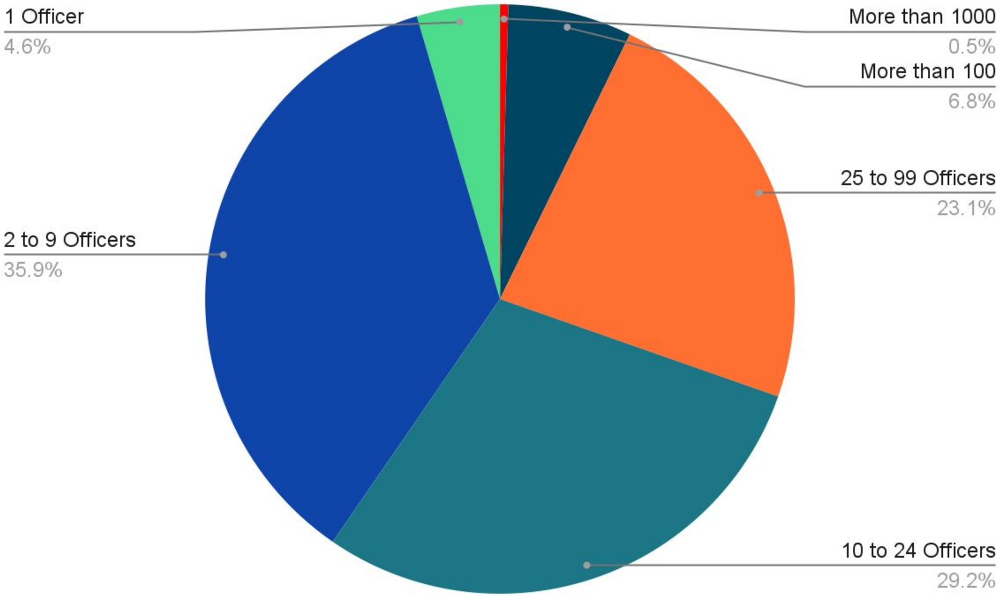
America’s Top Ten Biggest Law Enforcement Agencies



Evertas

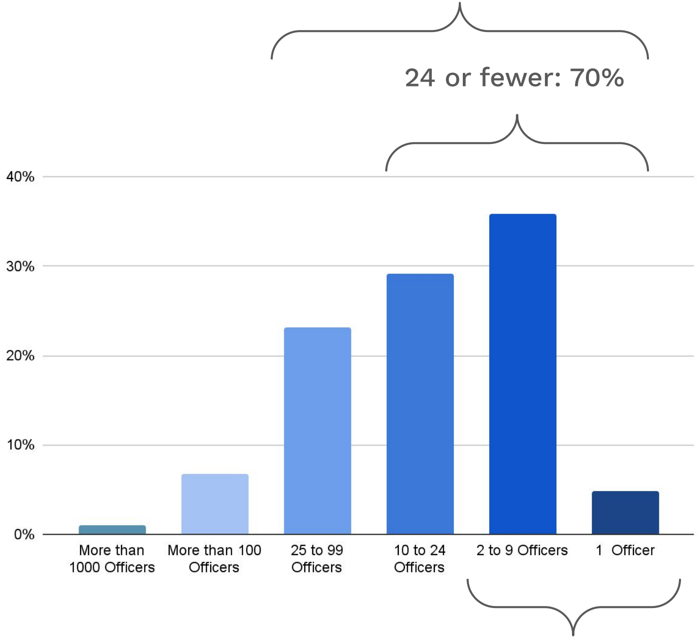
There are about 17,500 state and local police agencies employing at least one full-time sworn officer with general arrest powers

Law Enforcement Agencies by Number of Officers



99 or fewer: 93%

24 or fewer: 70%



9 or fewer: 41%

Bureau of Justice Statistics: Census of State and Local Law Enforcement Agencies, 2018 – Statistical Tables | Oct 2022

Local (& county, state, & tribal) Policing Really Is Local

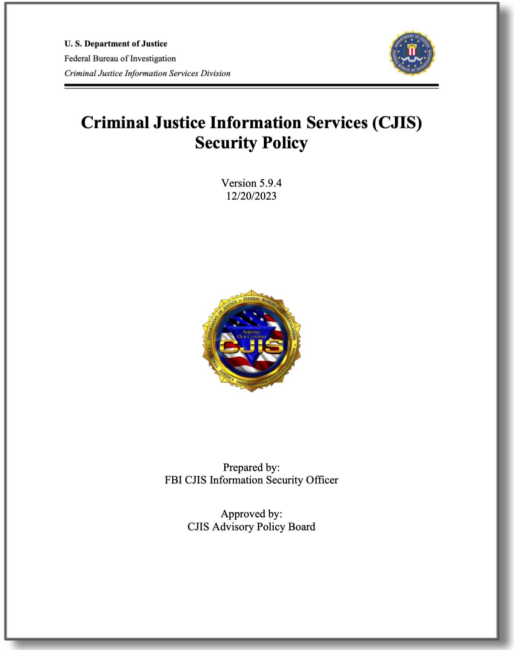
- The problems of the NYPD are different from, say, the New York Sheriff's Office. Both are different from the problems of Springfield (OH, or MA, or ...)
- My city’s budget for DPS: ~$1.89 million.
- NYPD budget: $10.8 billion

Top Three Cyber Challenges Facing Law Enforcement

- Identity and Access management
  - Who gets in, how do they get in?
    - Related: What gets in?
- Acceptable use
  - What can we do within the networks?
  - Who knows when this isn’t the case?
    - Related: who manages your network?
- Endpoint management
  - What is an endpoint, how is it managed?
  - Who owns the endpoint?
    - Related: does your department understand the liability of personal devices?

CJISSECPOL (*Gesundheit!*): Standards?

- Criminal Justice Information Services run nationally by the FBI
    - But each state has its own implementation.
    - It’s like PCI: “Approval” is murky, but fails are serious.
    - But it’s worse than PCI, because passing CJIS audit in TX is different from passing CJIS audit in Ohio or New York.
- It’s not a bad standard.
- It is 435 pages.
    - This is a usability issue.
    - This is an implementation issue.



U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS)
Security Policy

Version 5.9.4
12/20/2023

Prepared by:
FBI CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

Some High Level Problems

- M365 is the de facto standard. Out of the box, it's insecure and non-CJIS-compliant (e.g., MFA is <u>not</u> standard).
- Conditional access policies (trusted locations, etc), risky sign-in detection (velocity errors, etc.), come <u>only</u> with higher-cost "security" licenses like Office E5 or Entra ID P1.
- M365 spam filtering, identity impersonation protection, and link sandboxing are all also <u>not included</u> on lower tier plans.
- Departments across the country have not accounted for ballooning storage requirements. It's not just BWC video, it's everything.
  - Properly scoped storage allotments are expensive.
  - We can't throw anything away... Or can we?

Identity and Access Management

- Every cop’s password is their last name and badge/shield number.
  - OK, maybe not *every* cop. But lots.
- Many cops use that for usernames as well (Jones97, etc.)
- M365 access is not truly SSO and this is highly janky
- Some CJI data is highly personal (CCH, NLETS returns, etc.)
- The configurations are less than clear to ensure the person logging in isn’t in suburban Ouagadougou. As are those to help detect velocity conflicts (he logged in from his desk in Briny Breezes, FL at 9:02, and from Boring, OR at 9:03, etc.)

Acceptable Use

- Cops send everything by email.
- Really.
- Getting cops to understand the risk of sending sensitive data (CCH, DL photos, BOLOs, Intelligence Reports, CSAM, etc.) is seriously difficult.

Endpoint Management

- **If there is free AV, they will use it.**
  - If there is free *anything*, they will use it - when standards are federal but budgets local, we have a conflict.
  - True endpoint detection and response is *generally** only found in the 1%**.
  - If they click something — and they will — the detonation is often not controlled.
  - Gateway products to help sanitize mail, tools to stop, for example, obvious phishing, are needed and not included in cheaper M365, or frequently not configured.
- **Properly scoped endpoint and data backup is highly rare.**
- **Most cops still own their own portable devices**
  - This is an issue of national liability that Congress should solve
  - In addition to vulnerabilities, departments that mandate software create data breach risks for MOS/officers

* My city uses a MSP, NetGenius, of Arlington, TX whose principles have managed city and police IT for more than 15 years; one partner is a retired police detective.

** Mike Weiss, the Director of Technology for the City of Midlothian, TX, works miracles, but he is relentless and has a heart of stone and a constitution that is very, very rare. What a *gem* of a public servant - whatever they pay him, it is not enough.

Root Causes

- CISA's “best practices,” CJIS guidelines, NIST docs don't talk about prioritization in implementation…
- We Still Don't Capture True Cyber Crime Statistics
    - IC3 is not useful in terms of training cops to defend themselves or others
        - This is truly “a cyber hard problem”

Cyber Crime Investigation? No.

- Five years after the Cyber Enabled Crime pilot program at the NYPD, American local law enforcement doesn't have a strategy for cyber crime investigations.
  - With few exceptions, local cops still tell victims to “Call the FBI” or “There’s a website you can go to” then close the investigation locally.
    - By doing that, there are no statistics on local cyber crime victimization.
    - Also, no local victims see their case go to court, which means there is no case law, prosecutors, or victims’ rights groups saying, “We could have successfully prosecuted this crime with this change to the law...”
  - Local police must investigate cyber enabled crimes - they are fraud and extortion. But no training is available. Until cops see the volume in their city, no one thinks cyber is a big deal.
- Meanwhile identity theft reports are absolutely easy — this *can* be fixed.

* Cyber Enabled: Traditional crime abetted by cyber tools (e.g., fraud, larceny, extortion); or facilitated by use of cyber, like coordination or planning of traditional crimes using digital devices like phones or computers.

Root Causes

- Most agencies have no IT experience and low budgets.
  - Policing does not have a deep bench of cyber expertise. Often, is has none.
  - Culturally, cops – even the youngest cops – are not cyber-savvy. In fact, we have anecdotal evidence from the field that it is getting *worse*, as kids of the iPad age have never accessed a file browser.
  - The current generation of chiefs across the country still grapple with how cyber affects their workflow ("We didn't need computers when I was on patrol in the '80s" belies the importance of cyber to basic contemporary police work).
- Many agencies outsource all their IT to Managed Services Providers, few of which handle LE agencies.
  - This has led to breaches and ransomware.

Bottom Line

Something has to give when budgets are not unlimited, and education is lacking. In American non-federal law enforcement, that “something” is cyber security.

Without (a) dependable and objective cyber attack statistics, actionable intelligence, and cyber security prioritization, and (b) federal funding for local, county, state, and tribal law enforcement to implement all the CJIS guidelines, these problems remain intractable.

Questions?

nick@services.evertas.com

https://services.evertas.com

Tech Debt Burndown Podcast (Chris Swan & Nick Selby)

https://techdebtburndown.com