

November 29, 2023

Cybersecurity for Cities: A Bootstrapping Guide

Tech and Innovation Center Series
Local Infrastructure Hub



Tech and Innovation Center

Core Values

DRIVEN BY SHARED GOALS

Don't do tech for tech's sake. Priorities should be shaped through participatory processes.

DESIGNED FOR PEOPLE

Processes and products that reflect the needs of deeply diverse groups and individuals.

WELL- RESOURCED

Sustainable delivery systems with the workforce, policies, and agility to ensure effective regulation and integration.

BUILT FOR TRUST

Resilient solutions that are transparent, secure, available, reliable, durable, and privacy-conscious.



Cybersecurity is taking a growing toll: 2022 saw the largest-ever leak of personal data and record theft of digital assets

Hacker claims to have stolen 1 billion records of Chinese citizens from police

An anonymous internet user posted on the hacker forum Breach Forums last week offering to sell the more than 23 terabytes of data for 10 bitcoins, equivalent to about \$200,000,

U.S. Agency Links North Korea Crime Ring to \$540 Million Axie Infinity Crypto Hack

Lazarus Group has allegedly stolen nearly \$2 billion of crypto since 2017

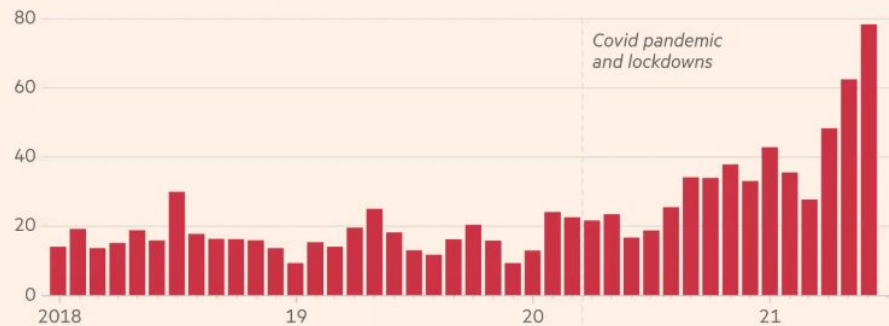
Why are we seeing more intrusions than ever?

- Security often not a primary consideration.
- Feature-rich systems may be poorly understood—combinations of features create unforeseen vulnerabilities.
- Implementations are buggy—e.g. buffer overflows, cross-site scripting.
- Networks are more open and accessible than ever, increasing exposure and making it easy to cover tracks.
- Many attacks are not even technical in nature—e.g. phishing, social engineering.

Cybercrime is economically-motivated, and easier than ever to monetize

Ransomware attempts reached an unprecedented level in 2021...

Global ransomware attempts (m)



...and bitcoin hit a record high

Bitcoin price (\$'000)



Sources: SonicWall; CoinMarketCap

© FT

Cities are on the front lines of cybersecurity

Every month in 2023 has seen major breaches of city cybersecurity.

Month	City	Type	Implication
January	Atlanta	ransomware	\$17m recovery cost
February	New Orleans	website bug	personal data on 100k residents
February	Oakland	ransomware	Phones + 311 down for weeks
March	San Francisco	payroll software	personal data on 70k employees
April	Chicago	City water billing software	personal data on 50k residents
May	Philadelphia	City health dept website bug	personal data on 40k residents
June	San Jose	ransomware	\$10m recovery cost

That
biggest-ever
data breach in
2022?

It was a city.

Hacker claims to have stolen 1 billion records of Chinese citizens from police

An anonymous internet user posted on the hacker forum Breach Forums last week offering to sell the more than 23 terabytes of data for 10 bitcoins, equivalent to about \$200,000,

2022 - SHGA Shanghai Gov National Police database
By ChinaDan - Thursday, June 30, 2022 at 08:55 AM

June 30, 2022, 10:15 AM (This post was last modified July 9, 2022, 10:22 AM by Staff. All threads locked by staff due to all the spam.)

In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB of data and information on billions of Chinese citizens.

Self: Shanghai GOV (SHGA.gov.cn) National Police Database
Host: <http://ops-cn-shanghai-shga-d01-a.ops.ga.sh/>
Data leaked from these tables:

-----TABLES-----
person_address_label_info_slave @y02584713e08c8e25ae 96 @ 588348916 @ 172.2gb 172.7gb
sh_theme_address_merge_tracks_slave -8aM81u8h8ubq2p8pA 360 @ 37482779389 @ 22.4tb 22.4tb
sh_theme_address_case_ded_text 7025d01700-1946a8d2 50 100 @ 2237506 1749387 25.7gb 25.7gb
sh_theme_address_company_ded_text 69ed780318e0c721e1a154 @ 1842506 @ 2.8gb 2.8gb
sh_theme_address_case_ded_text 7838a2a02a0f1g0d0d17g 154 @ 123413253 @ 31b 31b
sh_theme_address_company_ded_text 65f916102c035d00c02806 100 @ 2817981 @ 4.7gb 4.7gb
person_address_label_info_master 18c9c9b818a07211712a 36 @ 90880866 @ 282.4gb 282.4gb

Data Details:
Databases contain information on 1 Billion Chinese national residents and several billion case records, including:
- Name
- Address
- Birthplace
- National ID Number
- Mobile number
- All Crime / Case details

UPDATE: Per request, sample size increased to 750k (250k for each of the 3 main indexes): <https://gofile.io/d/eCggGC>
Staff update: Due to the chances of the file being reported to gofile, uploaded the sample to our own servers: https://cdn.breached.to/shga_sample_750k.tar.gz

PRICE: I am selling all of this data for 10BTC (\$200k USD)

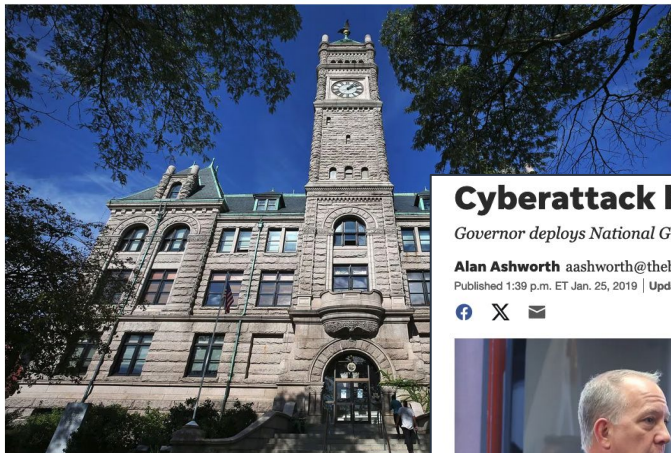
Contact for XMPP: dateman@rows.im

Edit: Locked by staff due to all the spam

Not just big cities

Hackers claim to publish data seized from Lowell in cybersecurity breach

By [Laura Crimaldi](#) Globe Staff, Updated May 14, 2023, 5:34 p.m.



Lowell City Hall in Lowell, Mass. DAVID L. RYAN/GLOBE STAFF

Cyberattack hits Akron

Governor deploys National Guard team to investigate ransom demand

Alan Ashworth aashworth@thebeaconjournal.com

Published 1:39 p.m. ET Jan. 25, 2019 | Updated 9:20 p.m. ET Jan. 25, 2019



Akron Mayor Dan Horrigan addresses the media during a news conference Friday at the Stubbs Justice Center. Standing with the mayor are FBI agent Bryan Smith, center, and Akron Police Chief Kenneth Ball. [Phil Masturzo/Beacon Journal/Ohio.com] *Akron Beacon Journal*

Why are cities
such good
targets?

Cities are good targets:

- mission-critical nature
- sensitive data holdings
- deep pockets

With lots of vulnerabilities:

- Aging IT infrastructure and legacy systems
- Inadequate staffing and skills
- Poor security practices (e.g. passwords, erasing discarded machines, etc.)

Federal and state resources for local government cybersecurity

The flagship cybersecurity program under the Bipartisan Infrastructure Law is the **State and Local Cybersecurity Grant Program**

- FY2023 funding is \$375m
- Only states and territories may apply
- 80% of its awarded funds must be passed through to local units of government, can be in form of in-kind services

Now is the time to:

- Check with your state SLCGP administrator for resource request procedures (e.g. [New Jersey](#)'s call is until through Dec. 8)
- Engage with state CISOs and coordinating agencies about needs and priorities for FY2024 (federal process re-starts in August 2024)

November 2023

Cybersecurity for Cities: A Bootstrapping Guide



Greg McCarthy

Chief Information Security Officer
City of Boston

Co-founder and Co-chair, Coalition of City CISOs



Dr. Brian Gardner

Chief Information Security Officer,
City of Dallas

The next Tech and Innovation
Center Series webinar will be
on December 13, 2023.