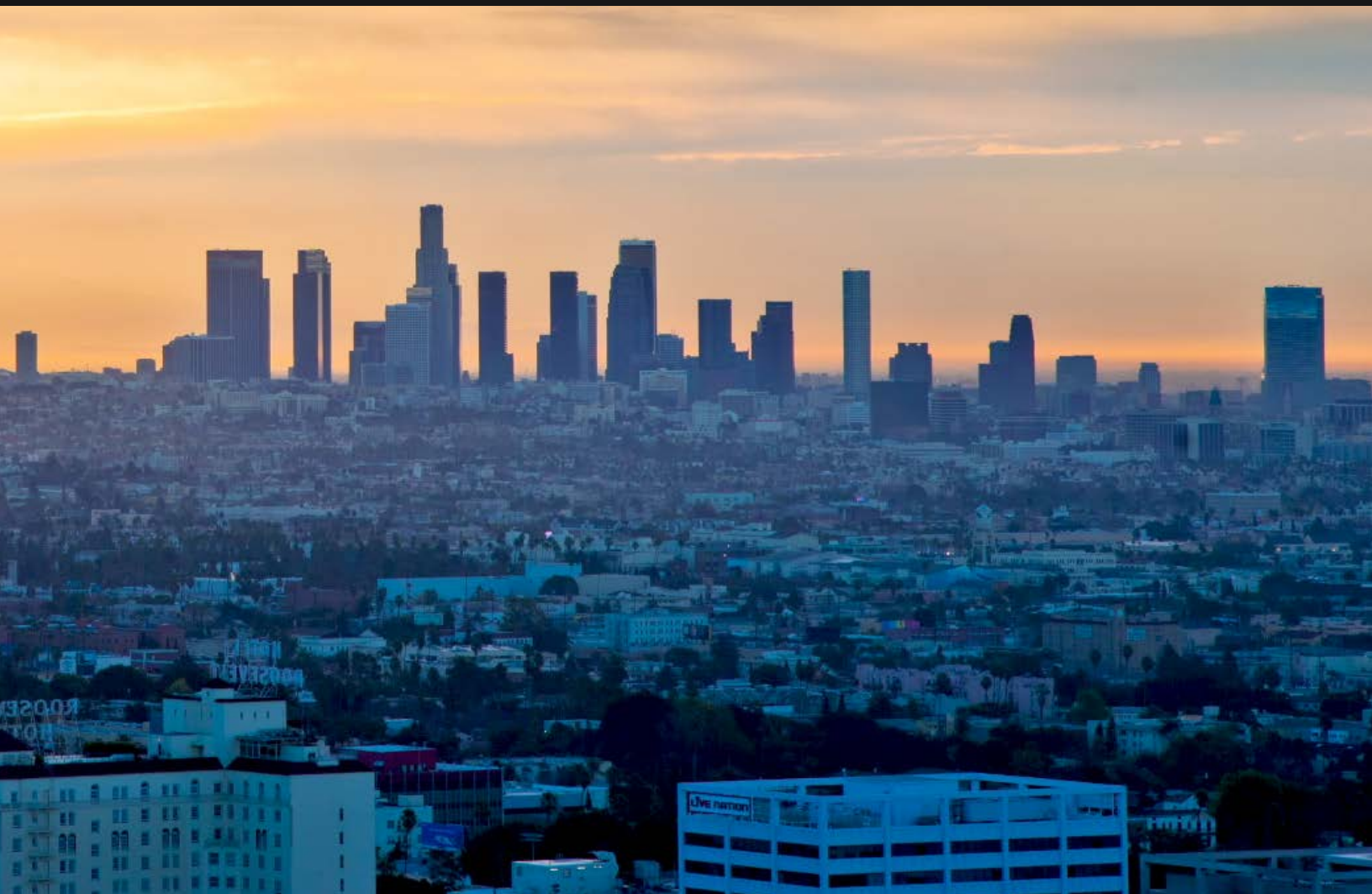
Safer citizens, stronger communities

Los Angeles partners with IBM Security to create first-of-its-kind cyberthreat sharing group



Simplify threat intelligence sharing

Protecting the community from online crime

The concept of information sharing to combat physical crime has existed for decades, long before the birth of the internet. As the virtual world evolved, it brought along an unwelcome guest: the cybercriminal. The same threat-sharing mindset that can provide an edge against crime in the real world was brought to life in the cyber world, as well, with multiple organizations springing up to better protect companies (and their customers) from online criminal activity.

Now that philosophy has leaped even further with the development of the Los Angeles Cyber Lab—an online community that combines the power of shared threat intelligence from private industry, government organizations, and everyday citizens. The result: a first-of-its-kind powerful arsenal that better protects business, public sector agencies and Los Angeles residents from increasingly sophisticated cybercrime.

Los Angeles: an attractive target

The city of Los Angeles provides a host of services to citizens—from access to public records, permit and license applications, education, infrastructure, health and human services —to name a few. Many of these services, in part or in whole, have been digitized, providing easy access for citizens and businesses.

At the same time, digitization of public sector information provides a uniquely attractive lure for online predators, who often find the trove of unique data held by state and local agencies fetches a lucrative price—whether it's held hostage in a ransomware attack, or wholly appropriated and sold. The data held by the city of Los Angeles and surrounding metro areas—with its rich diversity of large corporations, expansive population, and high profile—makes it an attractive target.

When it comes to defending against a quickly changing threat landscape and rapid-fire, sophisticated attacks, data alone is insufficient for protecting large populations. However, threat intelligence, when cultivated from a vast pool of trusted contributors, has the potential to change the game quickly on cybercriminals. That data can be taken even further, curated and converted into meaningful knowledge—which means everyone can act quickly and decisively to prevent cybercrime.

"We wanted to help the business community by providing threat intelligence, and we realized that we needed to automate that, and we knew we couldn't do it alone.[1]"

— Joshua Belk,
Executive Director for the L.A. Cyber Lab

Facelessness of cybercriminals

Securing the Internet of Things is a challenge
When a physical crime occurs in city streets, law enforcement can quickly respond with myriad physical forces to help protect citizens and businesses. Crime investigators often have insight and physical evidence about a criminal's tactics and motives, allowing law enforcement to use that information for future crime prevention. In contrast, cybercrime often has no obvious or immediate indications of how an attacker breached a system and what data was stolen or destroyed.

As cybercrime continues to evolve, attackers have a never-ending supply of vulnerabilities to exploit or potential victims to target in social engineering attacks. Threat actors are an opportunistic group and have a catalog of thousands of vulnerabilities available for potential exploitation. However, scan and exploit attacks only accounted for roughly one third of the top access vectors for cyberattacks in 2019, according to the 2020 X-Force Threat Intelligence Index.[2] Other cyber criminals prefer stealing legitimate credentials through phishing attacks to gain access. The use of legitimate credentials enables attackers to hide in plain sight and makes detection even more challenging.

Without valid or trustworthy information, local businesses, communities and concerned citizens can be overwhelmed by an attack and look to

state, local and federal government agencies

to mitigate or investigate cybercrime

"Ransomware attacks have reached the point where governments need to place an importance on them and develop response plans, similar to how they handle states of emergency.[3]"

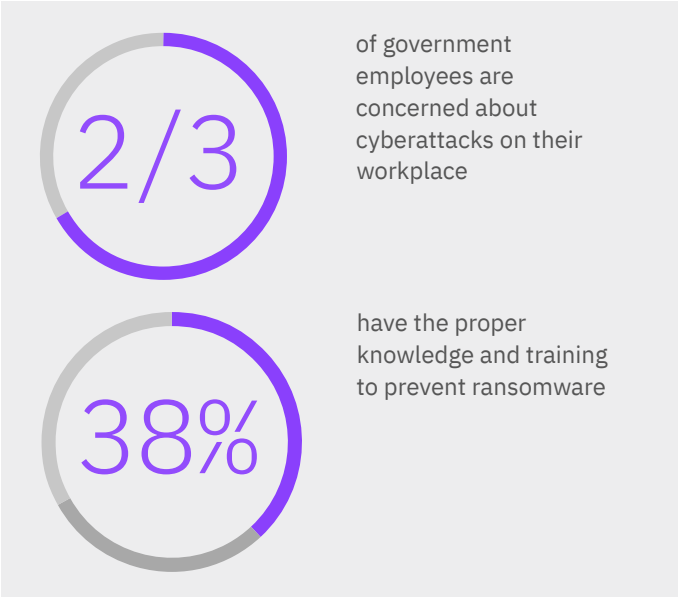
— Wendi Whitmore,
Vice President X-Force Threat Intelligence
IBM Security

Protect important assets

Government must keep data safe from online criminals while educating staff on preventative online behaviors

The 2020 X-Force Threat Intelligence Index identified government as the sixth-most attacked industry, up one rank from the seventh position it held in 2018.[4] Cyber criminals prefer to target the municipal or local level of government, since these organizations are less likely to benefit from the same level of cybersecurity funding as the private sector. Moreover, government entities hold valuable data assets spanning confidential state and financial information, critical network information, personal identifiable information (PII) and more.

Holding data hostage in exchange for money has become popular with hackers hoping to extort money — between January and July of 2019 alone, two-thirds of ransomware attacks targeted state and local governments.[5] A 2020 survey revealed that the human factor plays an important role in cyber defense: while two thirds of government employees are concerned about cyberattacks on their workplace, only 38 percent have the proper knowledge and training to prevent ransomware.[6]



"Ransomware attacks on government agencies continues to rise, and as victims pay attacker's ransom, they indirectly encourage both frequency and cost by making these attacks lucrative for cyberciminals.[7]"

— Wendi Whitmore,
Vice President X-Force Threat Intelligence
IBM Security

Build threat sharing communities across sectors

Using intelligence and technology to gain an edge against attackers

The city of Los Angeles, the LA Cyber Lab and IBM Security X-Force Threat Intelligence team joined forces to respond to citizens' expectations and bring threat intelligence to vulnerable local businesses. The partnership enables the sharing of unique threat insights about cyberattacks, business email compromise (BEC) data and phishing to assist government, businesses and residents in the Los Angeles area.

The creation of the LA Cyber Lab provides advanced capabilities to keep cyber-predators at bay. Because of the unique inclusive model—threat sharing between business, public agencies, and the public—it provides a layer of protection not seen in most municipalities.

- It is designed to improve the security and safety of businesses and citizens.
- It is built for action: the curated information creates better cybersecurity awareness and allows businesses and citizens to take action to better protect themselves.
- It is efficient: No singular entity alone could collect, pool, disseminate, verify and inform at-risk businesses and citizens.

Information sharing is facilitated by two tools available free of charge to residents and businesses in Los Angeles and nearby counties. One is a mobile application leveraging IBM Security threat intelligence to filter and analyze suspicious or potentially malicious emails. The second tool, and the centerpiece of this collaboration, is an innovative cloud-based platform—the Threat Intelligence Sharing Platform (TISP)—that functions as a digital neighborhood watch.[8]

How does TISP work?

TISP anonymously collects threat intelligence and other security information from volunteer organizations spanning city agencies, municipalities, critical infrastructure sectors and private companies. The platform uses artificial intelligence (AI) to analyze the data against a wealth of security information from IBM and generates threat intelligence and trend analysis for every member of the LA Cyber Lab.

For example, if a user submits a suspicious email, the platform reviews the email and extracts key information, then searches multiple common and unique data sources to indicate the level of risk. In addition to reporting the risk severity back to users, the platform has the capability to flag threat campaigns in the area, enabling both individuals and businesses to have an overall view of active threats.[9]

"The Threat Intelligence Sharing Platform and mobile app will advance the LA Cyber Lab's work that has made our city a national cybersecurity model, all while better defending Angelenos from cyber threats.[10]"

— Eric Garcetti,
Los Angeles Mayor

Craft resilient cybersecurity solutions

Community-wide collaboration serves both public and private sectors

Public and private organizations need to know what to do in the event of a cyberattack and they need to be resilient enough to withstand the aftermath. Many small and midsized businesses and government entities often don't have the option to suspend operations while defending themselves against malicious cyberactivity.

IBM X-Force brings to the table an advanced and integrated portfolio of enterprise security products and services. Leveraging insight from 800 TB of threat activity data, information on over 17 million spam and phishing attacks, real-time reports of live attacks, reputation data on nearly 1 million malicious IP addresses from a network of 270 million endpoints, [11] IBM X-Force provides users with valuable insight needed to prevent and combat modern day threats.

The public-private partnership between the city of Los Angeles, the LA Cyber Lab and IBM enables the city to fulfill its key obligation of protecting residents and businesses while facilitating crucial insight into threats that pose significant harm to both government and the community. This solution holds the promise of not only protecting residents and otherwise vulnerable enterprises, but also increasing the city's attractiveness for new businesses.

This new inclusive level of collaboration is a benchmark that can be emulated by cities and townships across the United States and beyond.

IBM X-Force strengths

800 TB of threat activity data

Information on over 17 million spam and phishing attacks

Real-time reports of live attacks

Reputation data from a network of 270 million endpoints

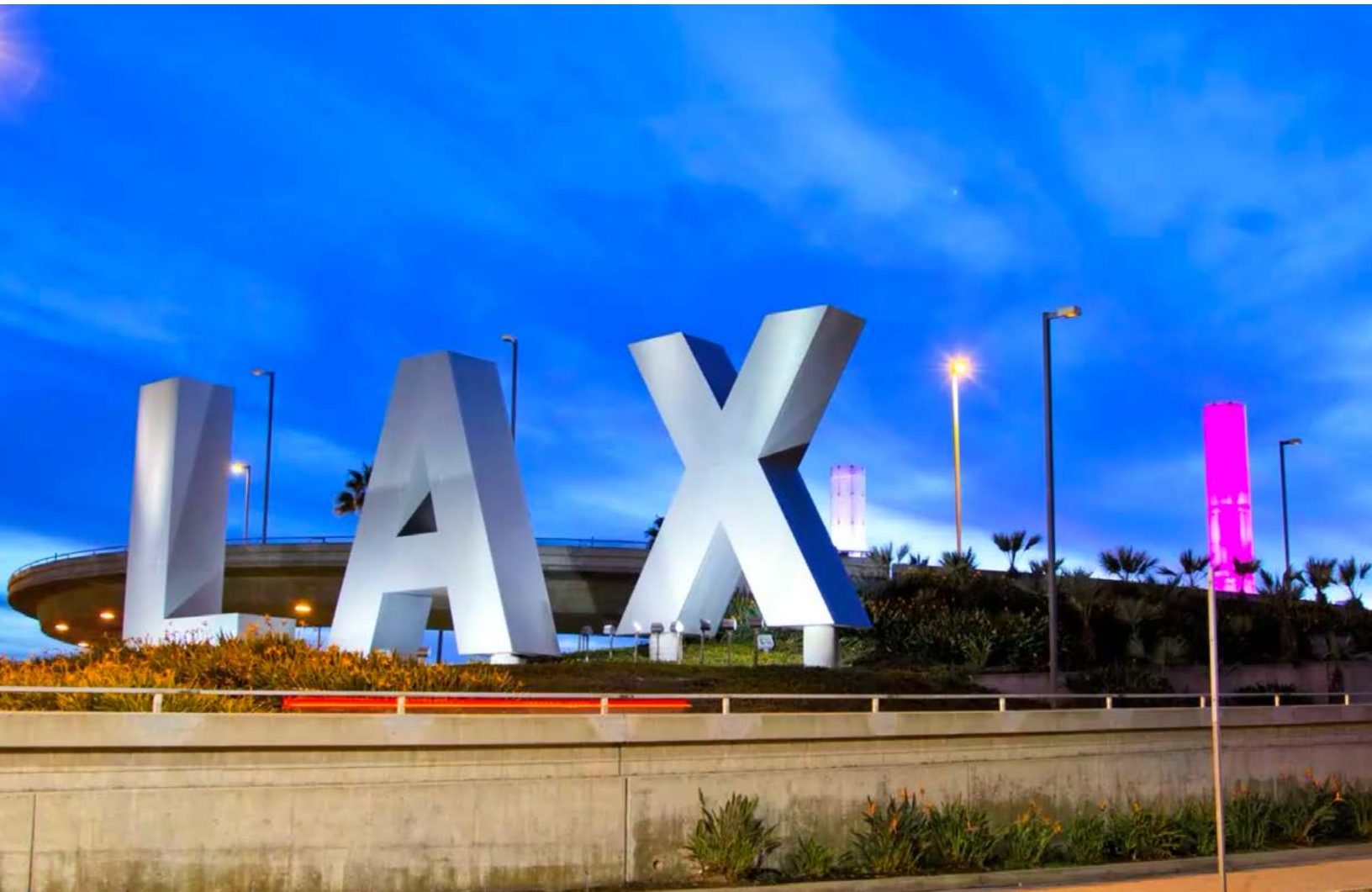
Next steps

Empower communities against cybercrime
Explore industry-leading security solutions built to help public and private sector organizations thrive in the face of cyber uncertainty.

Visit Security page – ibm.com/security/x-force-iris

Modernize government with technology
Discover tools and technologies that kickstart digital transformation and help governments deliver services that meet public expectations.

Visit Government page – ibm.com/government



References

1 Lucas Ropek. “L.A., IBM Launch Threat Intelligence Platform for Businesses” Govtech.com, September 18, 2019. https://www.govtech.com/security/LA-IBM-Launch-Threat-Intelligence-Platform-for-Businesses.html

2 IBM X-Force Threat Intelligence Index 2020 https://www.ibm.com/security/data-breach/threat-intelligence

3 IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks https://www.prnewswire.com/news-releases/ibm-security-study-taxpayers-oppose-local-governments-paying-hackers-in-ransomware-attacks-300912147.html

4 IBM X-Force Threat Intelligence Index 2020 https://www.ibm.com/security/data-breach/threat-intelligence

5 Fleming Shi. “Threat Spotlight: Government Ransomware Attacks” Barracuda.com, August 28, 2019 https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/

6 IBM Survey: Only 38% of State and Local Government Employees Trained on Ransomware Prevention https://newsroom.ibm.com/2020-02-27-IBM-Survey-Only-38-of-State-and-Local-Government-Employees-Trained-on-Ransomware-Prevention

7 IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks https://www.prnewswire.com/news-releases/ibm-security-study-taxpayers-oppose-local-governments-paying-hackers-in-ransomware-attacks-300912147.html

8,9,10,11 IBM Works With City of Los Angeles to Combat Cybercrime https://newsroom.ibm.com/2019-09-17-IBM-Works-With-City-of-Los-Angeles-to-Combat-Cybercrime

IBM Corporation
New Orchard Road
Armonk, NY 10504

81033381USEN-00