Cybersecurity for Smart Cities: Myths and Solutions

Convened by the

Technology and Entrepreneurship Center at Harvard

citypossible™ | Pioneered by Mastercard

During this year's Smart Cities CIO Summit at Harvard, convened by The Technology and Entrepreneurship Center at Harvard and made possible by City Possible by Mastercard, city leaders and executives from the technology sector came together for a meeting of the minds regarding a hot topic and rising problem for cities—cybersecurity.

Ransomware has become an epidemic among cities because they are not investing enough in cybersecurity. These attacks focus a great deal of attention onto databases, simply because the most valuable information is stored there.

A staggering 621 U.S. government, schools, and healthcare entities have been impacted by ransomware attacks since January of 2019, according to Emsisoft. Prior to that, in 2018, a massive ransomware attack launched by Iranian hackers shuttered Atlanta's city hall for five days. Additional attacks have been experienced worldwide in Canada, Ireland, and Sweden, just to name a few—targeting cities with outdated technology and infrastructure.

From January 13-14, 2020, CIO Summit attendees engaged in informative case studies, peer-to-peer problem-solving sessions, workshops, and exercises related to improving security in a digital age.

You can view all the presentations on the City Innovators Forum website here.

5 Myths of Cybersecurity

Presented by Simon Hunt, EVP of Cybersecurity Protocols at Mastercard

Myth #1: Hackers Only Target Businesses

Fact: Hackers target everyone—even cities—using robo hacks.

Whether you're the world's largest bank or the internet's smallest blog, automated systems mine the internet for vulnerabilities and don't care who has them.

Several U.S. cities were attacked by ransomware in 2019, closing down government phone and email systems. Hackers are taking a particular interest in Florida at the moment because three cities have paid the ransom thus far.

"All it took was three cities [in Florida] deciding to give money to criminals," explained Simon Hunt, EVP of Cybersecurity Protocols at Mastercard. "All the other criminals are saying, 'well maybe we should attack the same cities again because they have a history of paying. [Plus] what about their peers? Maybe their peers are no better or worse.'"

This sentiment echoed warnings from the FBI, who in an October PSA said, "paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals."

In at least two cases of municipality attacks in 2019, the ransomware was released through an infected email attachment. Other cities impacted last year included Baltimore, Maryland; Boston, Massachusetts; Gale, California; and New Orleans, Louisiana.

Myth #2: Hackers Are Geniuses

***Fact:** Hackers don't need intelligence when we give them everything they need.*

Successful hackers don't have to be smart, just diligent. Finding out how to exploit cybersecurity flaws is surprisingly easy, Hunt explained. You can literally search the internet, find vulnerabilities and buy your attack of choice for surprisingly little money. Robo hacks do the rest.

In fact, there is a search engine, just like Google, that you can search for specific pieces of code on a website - publicwww.com. If you know what you look for, you can find vulnerabilities in an instant. Another website on the dark web will tell you which sites to hack based on those results, making anyone a bonafide "hacker" in a matter of minutes. "We willingly give hackers an open door and because they have robo hacks that discover these things, they can just come and get them," said Hunt.

The truth is that nearly all "hackers" are lazy. They sit back and let the programs do the work, and sell those programs to other wannabe hackers to fund their criminal enterprises.

> ***"We willingly give hackers an open door and because they have robo hacks that discover these things, they can just come and get them."***

Simon Hunt, *EVP of Cybersecurity Protocols at Mastercard*

Myth #3: Hackers are Admirable/Cool

Fact: Hackers are common criminals that support some of the worst enterprises in the world.

We've all seen the trope—starving, brilliant hackers wearing hoodies in the movies and on TV. They're all just misunderstood loners, right? Wrong. In reality, these criminals profit from fraud, sexploitation, and destroying people's lives.

Marcel Lasar is spending four years in a Romanian prison for hacking celebrities and politician emails for blackmail and exploitation. Maksim "Aqua" Yakubets, meanwhile, is hiding in Russia from the FBI after defrauding consumers out of over $100 million.

Zachary Buchta, just 20-years-old, is headed to prison, as well. This hacker for hire co-founded Lizard Squad, a criminal organization behind DDoS attacks, bomb threats, and relentless harassment. Ironically (please refer to Myth #2), Buchta used his known screen name to call FBI agents "idiots" that are incapable of catching hackers.

In at least two cases of municipality attacks in 2019, the ransomware was released through an infected email attachment. Other cities impacted last year included Baltimore, Maryland; Boston, Massachusetts; Gale, California; and New Orleans, Louisiana.

The truth is that nearly all "hackers" are lazy. They sit back and let the programs do the work, and sell those programs to other wannabe hackers to fund their criminal enterprises.

Myth #4: Hacking is a Victimless Crime

Fact: Ransomware funds organized crime and costs citizens $600 billion per year.

Hacking is not only disruptive and costly but can be physically harmful to victims. This past year, three hospitals in Alabama were unable to use their computers and had to turn patients away. Seven hospitals in Australia also reported disruptive ransomware infections.

Roughly 60% of the $3.3 billion social media cybercrime industry is spent on manufacturing illegal and counterfeit pharmaceuticals, which kills tens of thousands of victims every year.

In December, the St. Lucie County Sheriff's office in Fort Pierce, Florida was taken offline by hackers—disabling email servers as well as the fingerprinting and background check systems.

Ransomware isn't just a mere inconvenience, it can result in tragedy and destroy lives for generations to come. Several people—including teenagers—worldwide have committed suicide after receiving ransomware threats. In one tragic instance, a man killed himself and his four-year-old son.

For consumers, it may be tempting to pay $100 to a hacker in order to get precious data like baby pictures back. However, there is no guarantee the files will be released back to you. In addition, that money goes directly into more organized crime like drug manufacturing, gun-running, prostitution, human trafficking, and of course, more cybercrime.

Myth #5: The Good Guys Can't Win

Fact: Anyone can guard against the most common attacks.

As we've already established, a majority of ransomware and other hacking attacks occur because it's painfully easy to find online vulnerabilities and take advantage of them. Taking basic steps to improve your cybersecurity can close a lot of these doors for hackers.

Hunt likens tightened cybersecurity to the one house on the block with a security system sign. If you're the only one on the block with a sign, no one will burgle you. But if everyone has a sign, you need the system.

The point of cybersecurity isn't to have the best security, just not the worst. As in nature, you don't have to be the fastest.

Don't be the slowest rabbit.

How to be a Faster Rabbit:

During his presentation, Hunt demonstrated security assessment program RiskRecon, a startup acquired by Mastercard that uses publicly available data to build security assessments of organizations.

As an experiment, Hunt assessed all the cities represented at the CIO Summit and presented the results with city names obscured. Many of these organizations were found to have serious vulnerabilities ranging from web encryption to web applications being used.

Mastercard is offering assessments to city leaders to help prevent ransomware attacks before they happen.

LINK OR CALL TO ACTION FOR MASTERCARD?

Request a Demo

riskrecon
mastercard

“

“It doesn’t matter how many layers of technology you put in place and how robust your cybersecurity implementation is if you have a user that clicks in the wrong place and gets you compromised.”

Cybersecurity Use Case: San Jose, California

Presented by Marcelo Peredo,
Chief Information Security Officer, City of San Jose

As the “capital of Silicon Valley,” San Jose, California plays host to over a million residents and 85,000 businesses, as well as infrastructure spanning 180 square miles. Ransomware attacks are being felt all over the country and municipalities have proven to be a “soft target” - that is, easy to identify weaknesses for and attack.

San Jose took a serious look at this problem and created a dedicated cybersecurity office in late 2018. At the time, the U.S. tech hub was weak in cyber controls, lacked a security framework, and identified numerous other concerns that needed to be addressed.

In addition to its new cybersecurity office, San Jose now utilizes a NIST cybersecurity framework, CMMI security maturity model, NSA’s Defense-in-Depth information assurance concept of layering security protocols, follows NIST guidelines for the Internet of Things (IoT), and intelligence sharing.

San Jose follows a five-step procedure to analyze and improve security:

1. **Identify** assets, conduct risk assessments, and create a risk management strategy.
2. **Protect** those assets through awareness and training, data security, proper maintenance and access control, etc.
3. **Detect** anomalies and incidents.
4. **Respond** with the protocols you have planned and trained for, analyze the problem, mitigate damage, and improve the process wherever possible.
5. **Recover** by communicating and improving.

Moving forward, Peredo says that his team will focus on patching, upgrading legacy software and other cybersecurity support. A major part of this plan, he said, involves training staff and making security a part of everyday habits.

“It doesn’t matter how many layers of technology you put in place and how robust your cybersecurity implementation is if you have a user that clicks in the wrong place and gets you compromised,” said Peredo

Moving forward, Peredo says that his team will focus on patching, upgrading legacy software and other cybersecurity support.

Panel: Cities Identify Their Most Urgent Cybersecurity Threats

Experts were invited to share what they considered to be the biggest risk in cybersecurity right now, as well as recommend solutions for them.

Marcelo Peredo, Chief Information Security Officer of the City of San Jose, said that more than ransomware, he sees a real problem with business email compromise.

"[Hackers] get a hold of an account and they wait for the right moment to make the right interaction to intercept the payment of an invoice or the exchange of sensitive information. And that's when the payoff takes place," said Peredo. "We experienced one that, lucky for us, was not that of a significant amount. But in resolving that situation, I learned that it's actually paying a lot more than ransomware to the bad guys."

Chris Seidt, Director of Information for the Louisville Metro Government in Kentucky, said that vulnerabilities exist first, and foremost, with the user. Seidt echoed Peredo's sentiment regarding business email compromise, stating that several of Louisville Metro's partners will receive an email from a legitimate source, but the request is out of the ordinary.

"A nonprofit organization might ask to have a meeting with you... or ask for a financial commitment," said Seidt. "They're not going to ask you to go out and buy them a prepaid cell phone. I think there's still an opportunity to train people beyond 'this is a phishing email.'"

Celeste O'Dea, Oracle's Business Development Director of PS Technology for Federal and Canada Applications, noted that data security is the biggest exposure threat for cities.

"Data analytics is becoming even more critically important in everything," said O'Dea. "[With all] the data that's being generated by IoT sensors, open Wi-Fi access, and migration to the cloud, [probably your biggest threat] is the ability to breach through those various mediums and get to the data that is critical to your operations."

Simon Hunt, EVP of Cybersecurity Protocols at Mastercard, agreed that users are the first line of defense against attacks.

"Our users and community are not part of the fight with us," said Hunt. "How many of you use the same password on more than one website? The problem is that we are lazy but the hackers are a little less lazy. Somehow over the 30-year history of cybersecurity, we still haven't got the basic education in place and we still don't have the population helping us in this fight against the criminals. The biggest threat is that we continue [to become] more digital and yet our employees are not a part of this endeavor with us."

Mark Wheeler, Chief Information Officer for the City of Philadelphia, noted that some analysts across the city government, especially in health and human services, do not take the cybersecurity training provided. As a result, these departments will take approved platforms but add data to them that becomes exposed to the public.

"Our HIPAA is mandatory and our cybersecurity is mandatory," Wheeler stressed, "and I think for analysts, we're going to have a third component that's specific for them."

> ***"How many of you use the same password on more than one website? The problem is that we are lazy but the hackers are a little less lazy." - Simon Hunt."***

City Leaders answer: What is the biggest security threat to cities at the minute?

- He threat to be ransomware, now business email compromise.
  Marcelo Peredo, San Jose
- He threat people and training problem, people need to know "What is the norm and What isn't? Why would this person ask me to send them money out of the blue?"
  Chris Seidt, Louisville
- He threat users, education for the population.
  Simon Hunt, Mastercard
- He threat Data problem, users first line of defence they are the first weakness.
  Mark Wheeler, Philadelphia

Tools of the Trade

Panelists shared tools they currently use to detect and combat cyberattacks:

- **Darktrace:** an AI-powered service that detects activities outside out of normal activity
- **CrowdStrike:** a cloud-based endpoint protection platform

The experts then shared a few suggestions for mitigating risk:

- **iPads** A number of city representatives claimed to use or be in the process of transitioning from PCs to iPads for their portability and Apple's lack of malware. However, the high price of iPads and the inability to run PC-based firewalls prevent widespread adoption at this time.
- **Patch, patch, patch!:** Keep programs up to date for the latest security features.
- **Perimeter Security:** Even reactive security can stand between you and attacks.
- **Incident Command Training:** The U.S. Department of Homeland Security offers free cybersecurity training called the National Incident Management System (NIMS). Management staff for Louisville Metro Government went through the training, and frontline staff will take it, as well. Grants are available for advanced NIMS training.
- **Redundancy and back-ups:** The impact of ransomware lessens significantly when you can restore information easily on your own.

Workshop: Top 10 Things Cities Need to Address to Improve Cybersecurity

Following the cybersecurity panel, attendees were split into groups of five and asked to pick their list of top ways to improve their own security. All groups submitted their top items and then people voted for their favorites.

Here, in no particular order, were the top 10 items that city leaders identified as areas of improvement in cybersecurity:

1. **Education** - staff needs to be educated on a regular basis on how to spot threats/phishing, etc.
2. **Patch** - cities need to patch new software to close known security gaps.
3. **Don't use legacy systems** - This one seems obvious, but systems that aren't supported anymore e.g. Windows XP, are still being used in cities, providing an easy way in.
4. **Have a strong 'response plan'** - When the city is attacked, ensure everyone is well briefed on exactly what to do. Treat this plan as a fire drill - practice and keep everyone ready to leap into action.
5. **Have a communications plan** - Have a narrative to share with media in advance, because you will not have time to construct this when an attack happens.
6. **Have an IT inventory** - ensure you know everything that is connected to your systems and what software they are running.
7. **Establish a strategic partnership with a cyber attack agency** - think of this as the fire brigade - when the building is on fire, you know who to call and they can see a list of who is in the building, giving them the tools to strategize.
8. **Conduct regular risk assessments** - stay ahead of problems.
9. **Formalize interlocal agreements** - neighboring local authorities and cities can help when attacks happen. Discuss this with them in advance, however, not after attacks happen.
10. **Privilege Analysis** - What 'access' or 'privileges' should staff or applications have in your systems?

The CIO/Smart City Leader summit brings together the top leaders in cities across the globe to discuss the key issues, ideas, and opportunities for 2020. This invitation-only program was co-developed by the Fellows from the Technology and Entrepreneurship Center at Harvard along with city leaders and industry expert partners.

To learn more, please join us on the City Innovators Forum website.

Convened by:

Technology and Entrepreneurship Center at Harvard

In partnership with:

citypossible™ | Pioneered by Mastercard