

# ICIT'S BRIGHT MINDS Q&A SERIES

---



## Smart City (In)Security

with

CESAR CERRUDO, CTO IOACTIVE

December 2019

---

## Bright Minds Q&A

# Smart City (In)Security

With Cesar Cerrudo, ICIT Fellow and CTO, IOActive

December 2019

---

Copyright 2019 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the [www.icitech.org](http://www.icitech.org) website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

## **About This ICIT Bright Mind Q&A**

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing the cybersecurity community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations.

Critical infrastructure is increasingly dependent on smart city and Internet of Things (IoT) devices. However, many of those systems were not designed with security features, and some cannot be secured at all. Adversaries can leverage vulnerabilities in [unsecured IoT devices to laterally compromise sensitive systems](#), [disrupt business operations](#), or [jeopardize public safety and security](#).

With an estimated 200 billion IoT devices connected to the Internet and an estimated global market exceeding one trillion dollars by 2020, digital adversaries will target and compromise vulnerable IoT devices because the threat landscape is lucrative. To protect smart cities and all connected networks and systems, IoT devices must be developed with security by design throughout the development lifecycle.

In this Bright Minds Q&A, ICIT Fellow and IOActive CTO Cesar Cerrudo explains the problematic culture contributing to insecure smart city environments and he recommends measures to improve smart city cybersecurity, protect public infrastructure, and mitigate threats to critical infrastructure.

### **About this Bright Mind: Cesar Cerrudo, CTO of IOActive, Inc.**



Professional hacker, cyber security futurist and entrepreneur.

Currently, Cesar is Chief Technology Officer for IOActive Labs, where he leads the team in producing ongoing, cutting-edge research in areas including Industrial Control Systems/SCADA, Smart Cities, the Internet of Things, Robots, Blockchain, Cryptocurrencies, and mobile device security. Cesar is a world-renowned cyber security researcher with more than 15 years of experience.

Throughout his career, Cesar is credited with discovering and helping to eliminate dozens of vulnerabilities in leading applications including Microsoft SQL Server, Oracle database server, IBM DB2, Microsoft Windows, and Twitter. He has a record of finding more than 50 vulnerabilities in Microsoft products including 20 in Microsoft Windows operating systems. Based on his unique research, Cesar has authored white papers about cyber security problems, attacks, and exploitation techniques in different widely used technology. He has presented his research at a variety of company events and conferences around the world including Microsoft, Intel, Black Hat, Bellua, CanSecWest, EuSecWest, WebSec, HITB, Microsoft BlueHat, EkoParty, FRHACK, H2HC, Infiltrate, 8.8, Hackito Ergo Sum, NcN, Segurinfo, RSA, and DEF CON.

He started [Securing Smart Cities](#), a non-profit initiative to make world cities safer, after he found that most Smart City technologies are vulnerable to cyber-attacks.

Cesar collaborates with and is regularly quoted in print and online publications. His research has been covered by Wired, Bloomberg Businessweek, TIME, The Guardian, CNN, NBC, BBC, Fox News, The New York Times, New Scientist, Washington Post, Financial Times, The Wall Street Journal, and other leading publications.

He works hard to make the world a more secure place.

Cesar is also CEO and founder of Argeniss Software, boutique software development company.

**ICIT:**

The potential market for smart devices is projected to exceed one trillion dollars and over 200 billion devices by 2020. Given the size and scale of the potential market and the predicted pervasiveness of smart city devices, what are some examples of current risks and attack vectors that municipalities are not prepared for as part of the new digital society?

**Cesar Cerrudo:**

There are many risks associated with rapid smart city technology adoption. Most municipalities are acquiring technology and deploying it without any security testing, blindly trusting the vendors. They do a lot of functionality testing to ensure the technology is the best solution, but security testing is usually non-existent. This means that insecure technology is installed, leaving the municipalities open to cyber-attacks and putting their stakeholders at risk for the related consequences. It's important that municipalities always test the security of new technology either using their own teams or a third party. They could also ensure technology contracts require vendors to provide secure technology and put sanctions in place if security problems arise. This won't stop the municipality from being open to cyberattacks, but it could help to reduce losses when one occurs.

**ICIT:**

Are smart city systems built with security by design? If not, why are devices being adopted without proper security testing or having undergone secure lifecycle development?

**Cesar Cerrudo:**

Most smart city systems aren't built with security-by-design principles. As mentioned before, governments blindly trust vendors and are often fooled by them. Vendors always claim their technology is the most secure, but usually, it's just a marketing pitch because their security is really bad, lacking encryption, authentication, and authorization. When technology has encryption, authentication, and authorization, they usually are poorly implemented, making it very easy to bypass and thus almost useless. Sometimes vendors are asked by governments to fill out a questionnaire with security questions about the products, like: does the product use strong encryption, yes or no? Is the product using authentication, yes or no? Unfortunately, it is up to the vendor to tell the truth, since no-one checks the answers by testing the product. In other cases, there are good security policies in place for secure technology adoption, but they are not enforced, making them useless.

**ICIT:**

What are some of the most significant challenges in securing smart city infrastructure?

**Cesar Cerrudo:**

Smart city infrastructure is complex; it's a system of systems, where old technology lives with new technology. Gradually deploying a new technology while securely coexisting with legacy technology is a big challenge as legacy systems are more insecure. By coexisting, they make all the systems more insecure, including the new ones. For instance, patching legacy systems is sometimes impossible, requiring users to accept the risks until they can be replaced. Many communication protocols used by smart city technologies are not based on technological standards meaning only the vendor really knows if their protocols are secure. This is a threat as protocols can be reverse engineered and vulnerabilities discovered. Communications that use standard protocols are better as they can be easily examined, but this doesn't guarantee the implementation is secure. For this, you need to audit the implementations which is a challenge because governments don't have enough resources, skilled people, or money to properly audit the technology before acquiring it.

**ICIT:**

Cities often have limited budgets and often face a shortage of cybersecurity talent. Given these constraints, what can cities do to mitigate attacks and secure vulnerable infrastructure?

**Cesar Cerrudo:**

Partnering with local universities to help test the security of technologies can be useful, but doesn't scale well since universities lack real-life experience and also are limited by resources. It's key to think smart and assign the limited resources available to the most critical technology. Of course, this requires identifying which areas are the most important. Looking for third party help when possible is another good option as this leverages security companies' expertise, services, and software to audit and protect technology.

**ICIT:**

How can smart device manufacturers improve security and resiliency of devices before release, during installation, and after adoption?

**Cesar Cerrudo:**

They should implement a secure by design approach using a secure development lifecycle program. They should conduct a security audit on the technology with a third party. This will require developing a security playbook that covers all the procedures from when a security vulnerability is found to reporting where it is and how the fix is produced, tested, released, and applied. Additionally, it is beneficial to have a security response team that easily deals with security issues and is the point of contact when something happens. In this way, a company can be prepared to produce more secure devices and provide governments with a fast and good response when a problem arises.

**ICIT:**

What can regulators and lawmakers do to ensure that security is included in smart devices?

**Cesar Cerrudo:**

Currently, technology vendors have no incentive to produce more secure technology. Governments keep buying, they keep selling, and everything is fine. There should be strong policies, requirements, regulations, and laws in place to force vendors to be serious about security. For instance, governments could set high fines for non-compliance with basic security standards or require vendors to have their products certified by a security auditor before they can become a government provider. Regulation could force vendors to minimize security defects in products and follow security best practices. Also, using a trusted and secure supply chain should be enforced since many components are developed by third parties overseas, with the potential for products to have built-in backdoors and security problems.

**ICIT:**

Smart city inhabitants may feel helpless against ransomware or other digital attacks when the decision to rapidly adopt smart city technology is out of their hands. What recommendation do you have for everyday citizens who want to be part of the solution but are unsure how to get involved?

**Cesar Cerrudo:**

People should talk to their representatives and complain when they see the problems or face the consequences of unsecure technology. Being quiet means being part of the problem, so it's important to speak out and strive be heard, because otherwise everything will continue as usual.