IOT & Smart Cities
Cyber Security Threats and Defence

Chris Gibson, Executive Director

Forum of Incident Response & Security Teams

chris@first.org

FIRST™

Improving Security Together

Who am I?

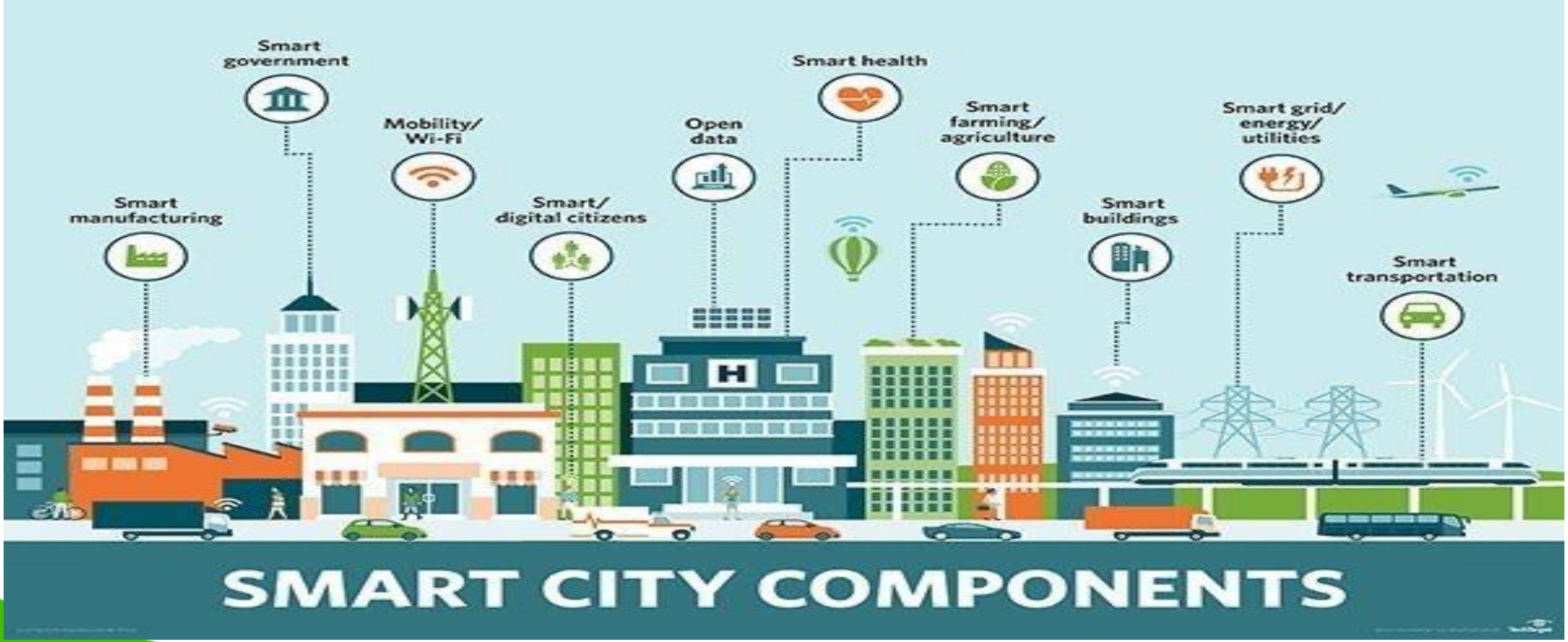
- Chris Gibson
- 19 Years at Citi, global responsibilities for incident management and computer forensics
- 10 Years on the board of FIRST.Org (5 years as CFO, 2 years as Chair)
- Built and ran CERT-UK, the United Kingdom's first formally chartered National CERT
- 2 years in financial services as CISO
- Recently started as Executive Director for FIRST.Org
- e: chris@first.org
- w: www.first.org

What is a “Smart City”

- A **smart city** is a municipality that uses information and communication technologies (ICT) to increase operational efficiency, share information with the public and improve both the quality of government services and citizen welfare.

https://internetofthingsagenda.techtarget.com/definition/smart-city

What does that mean?



How is it all joined up?

- Collection - Smart sensors throughout the city gather data in real time.
- Analysis - Data collected by the smart sensors is assessed in order to draw meaningful insights.
- Communication - The insights that have been found in the analysis phase are communicated with decision makers through strong communication networks.
- Action - Cities use the insights pulled from the data to create solutions, optimize operations and asset management and improve the quality of life for residents.

And technically?

- mesh network
- machine to machine (M2M)
- cloud computing
- application programming interfaces (APIs)
- machine learning (ML)
- artificial intelligence (AI)
- dashboards

And what does that mean?

Complexity

What do we all know?

Marsh/Microsoft (2019)

- 88% said information technology/information security (IT/InfoSec) is one of the three main owners of cyber risk management, followed by executive leadership / board (65%) and risk management (49%).

- Only 17% of executives say they spent more than a few days on cyber risk over the past year.

- 83% have strengthened computer and system security over the past two years, but less than 30% have conducted management training or modelled cyber loss scenarios.

- Firms’ confidence declined in each of three critical areas of cyber resilience. Those saying they had “no confidence” increased:
    - From 9% to 18% for understanding and assessing cyber risks.
    - From 12% to 19% for preventing cyber threats.
    - From 15% to 22% for responding to and recovering from cyber events.

- There was a discrepancy in many organizations’ view of the cyber risk they face from supply chain partners, compared to the level of risk their organization poses to counterparties.
    - 39% said the cyber risk posed by their supply chain partners and vendors to their organization was high or somewhat high.
    - But only 16% said the cyber risk they themselves pose to their supply chain was high or somewhat high.

- 43% reported “no confidence” in their ability to prevent cyber threats from at least one of their third-party partners.

And that means?

- We consistently fail at doing the basics correctly
- We run before we can walk
- The pace of change outruns our ability to manage it

Real world benefits

- The City of Barcelona saved more than 75 million euros by adopting IoT-driven smart water, lighting, and more in 2014.
- Intel (March 2018) calculated that smart city technologies could give back 125 hours to citizens every year. If time is money, then that amounts to a significant sum: US$5 trillion annually. Successful smart city initiatives place improving citizens’ quality of life above money-saving, with the latter often being an indirect outcome.

So, what does this tell us?

- We need to significantly improve
  - Both in our technical ability to get it right first time
- But also
  - In our ability to cross the divide between tech and the business
- And also add in
  - Building trust across the whole piece

Do users trust complex systems?

Challenges

- Systemic Vulnerability
  - By integrating everything we potentially create a single point of failure
  - Significant effort will be required to ensure this is secure.

But what other challenges are there?

- Trust
  - The privacy implications of such a system are obvious.
  - **Significant** effort will be required to build and maintain trust across the whole enterprise.

How do you build trust in a smart city?

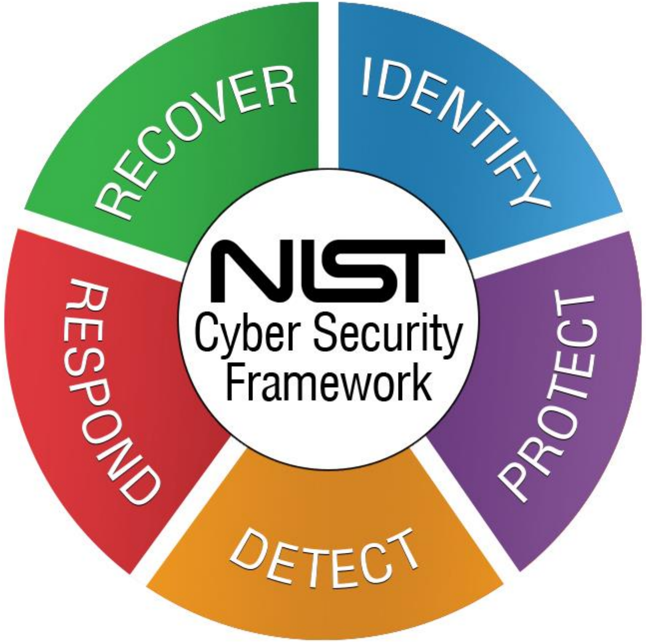
- The only way to build strong trust is by providing cost-efficient services that give real outcomes and allow residents and all others to rely on such services in their time of need. Consistency plays an important role in earning and reinforcing this trust.

What do you need to consider?

- People need to buy into it
- While it’s good to have a vision, realism is important.
- Cultural issues should be considered
- Do a small number of things extremely well, allowing for additional services

What are the implications?

- NIST Model



Identify

- How do we identify all the devices on the network?
  - Devices will come and go
  - Volume and capacity
- How do we collect logs?
  - In real time?
- How do we analyse the complex relationships?
  - And ever changing relationships?

Protect

- **Device Identification:** The IoT device should have a way to identify itself, such as a serial number and/or a unique address used when connecting to networks.
- **Device Configuration:** Similarly, an authorized user should be able to change the device's software and firmware configuration. For example, many IoT devices have a way to change their functionality or manage security features.
- **Data Protection:** It should be clear how the IoT device protects the data that it stores and sends over the network from unauthorized access and modification. For example, some devices use encryption to obscure the data held on the internal storage of the device.
- **Logical Access to Interfaces:** The device should limit access to its local and network interfaces. For example, the IoT device and its supporting software should gather and authenticate the identity of users attempting to access the device, such as through a username and password.
- **Software and Firmware Update:** A device's software and firmware should be updatable using a secure and configurable mechanism. For example, some IoT devices receive automatic updates from the manufacturer, requiring little to no work from the user.
- **Cybersecurity Event Logging:** IoT devices should log cybersecurity events and make the logs accessible to the owner or manufacturer. These logs can help users and developers identify vulnerabilities in devices to secure or fix them.

https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

Detect

- Correlating events across multiple data sources
  - In real time
  - Across multiple systems
- One MCERT entity or many?
- Complexity

Respond

- In real time
- Systems should be designed to be manually overridden should a hack or malfunction make it necessary to retake control.
- MCERT – again, one or many?
- And during this the DETECT mission must be fully operational

Recover

- You can’t “turn it off and on again”
- Must be well planned
- Prioritized
- And during this the DETECT & RESPOND mission must be fully operational

How can we address these challenges?

- Leadership
- Manage the information gap
- Build relationships
- Make sure you have the right skills
- Understand your obligations
- Exercise, exercise and exercise

Leadership

If an incident is significant, senior leadership response is critical. Management must coordinate with corporate communications, legal, audit and compliance teams, human resources, and technical staff. Incidents can be enormously complex. And, we've all seen incidents where executive mishaps, after the incident was discovered, lead to ethical and legal questions.

Proper leadership can help avoid such situations.

Manage the Information Gap

Plan ahead to have a communications lead, who works closely with the incident leader, and works to satisfy third party information requests from across the organisation. During an incident, there will be a large set of requests for information, with a small team actually investigating and developing the deliverables.

An often-overlooked piece is to record details of each decision as it happens.

Good communications through an incident can make ALL the difference between success and failure.

Build Relationships

When an incident strikes, it’s too late to build trust and relationships. Have your team engage with business partners, national CSIRTs and service providers before you need the relationship.

Join relevant organisations in the field, meet their security teams at conferences and industry working groups, or use existing mechanisms such as a vendor review process to determine and track the right points of contact early on.

Effective cooperation during an incident is ALL about trust.

Make sure you have the right skills

Retain external legal, PR and technical support. There will be technical skills not available to your team. These may include legal, public relations and technical support, such as crisis management or disk forensics.

Find a provider for these services and sign a retainer, BEFORE the incident strikes.

Understand your obligations

You may have made commitments to your customers on how quickly you'll inform them when an incident occurs. Even if you haven't, various reporting regulations are now in effect, such as the GDPR, where organisations typically have up to 72 hours to gather relevant information and report to the appropriate regulator – or the European Union NIS Directive, according to which specific Digital Service Providers must report "with no undue delay".

Understand ALL your requirements ahead of time, so your incident response process takes them into account.

Exercise, exercise, exercise

It’s a common misunderstanding that security exercises are only important once you’ve achieved a certain level of maturity. Take a scenario that affected another organisation and perform a table-top walkthrough of how your organisation would deal with that same incident. At the very least you’ll identify gaps you still have to address. Exercises should be regular and involve a range of participants. It’s important that the senior members of an organisation (right up to senior executive management members) as well as the technology and other staff participate.

The “muscle memory” this will build is invaluable when a real incident occurs.

Closing the circle

The most important phase when handling a incident is the “post-mortem”. It’s almost impossible to prevent all incidents from happening, so this is a chance to review why this one took place, and identify ways to improve your program. Ask the “Five Why’s”: every time you believe you have an answer to why the incident took place, ask for a deeper, underlying cause, until you hit at least five levels of “Why.”

Address all levels, and focus on the deeper, underlying ones, as they will lead to other, future incidents if left unaddressed.

Closing the circle

Never let a good incident go to waste. There are two positive benefits from an incident:

- The first is that as it so clearly illustrates both needs and impacts; an incident is often the best time to get additional investment to prevent the next one. Make sure to clearly communicate what your security program needs to be more effective and create follow up plans to get buy-in from senior leadership in your organisation.
- Secondly, every incident you work helps you learn more about your organisation; how your systems interact but more importantly, how your people interact.

How can FIRST help?

FIRST's Mission

Global Coordination: In an emergency you can always find the teams you need to support you in our global community.

Global Language: Incident responders around the world speak the same language and understand each other's intents and methods.

Automation: Let machines do the boring calculations, so humans can focus on the hard questions.

Policy and Governance: Make sure others understand what we do and enable us rather than limit us.

How can FIRST help?

Global Coordination: Every FIRST member can successfully find a FIRST member to work with during any incident, whether in another country or industry.

FIRST organized 4 Symposia, 11 Technical Colloquia and 11 training sessions (4 taking place during existing FIRST events around the world). These events are opportunities not only to exchange ideas and know-how, but also to grow trust and meet peers. Our events and training sessions would not be possible without volunteers, and we invite interested parties to contact us about opportunities to contribute.

Global Language: FIRST teams know they can rely on FIRST teams. FIRST members have a common understanding of methods and issues.

We are committed to ensuring that FIRST members can trust that other FIRST members meet a minimum level of capability. We will invest in training and education to ensure that knowledge sharing is effective, comprehensive and the same among all members.

How can FIRST help?

Automation: When FIRST members trust each other they have a toolset they can use to automate sharing.

To improve collaboration, FIRST supports its members in developing shared tools and standards so they can efficiently and reliably share information.

Policy & Governance: FIRST members can work in an environment that is conducive to their mission

As a member of the Internet Technical Community, FIRST continues engaging with policymakers and Internet governance bodies to provide technical expertise where appropriate. While FIRST does not engage in policymaking efforts, we do contribute to technical discussions contributing to the wider Internet governance debate. In particular, we educate policymakers and other stakeholder communities about the challenges of the Incident Response community.

IOT & Smart Cities
Cyber Security Threats and Defence

Chris Gibson, Executive Director

Forum of Incident Response & Security Teams

chris@first.org