KPMG

Smart Cities & IoT
– Trust and Resilience

June 2019

With you today

Jason Stevenson
Director, Cyber Security
T: 250 480 3531
E: jasonstevenson@kpmg.ca

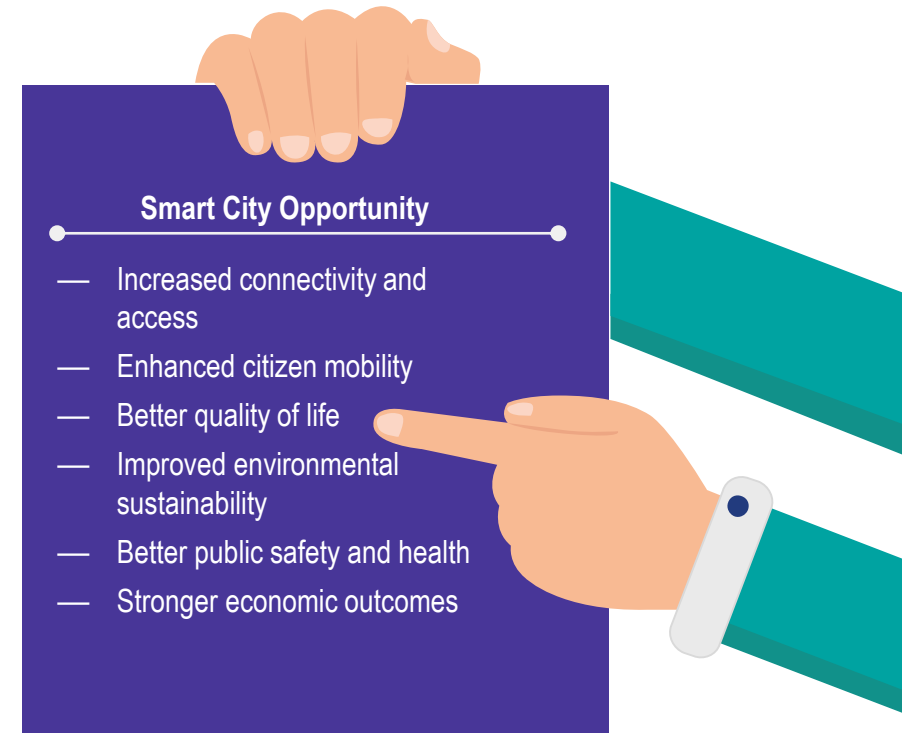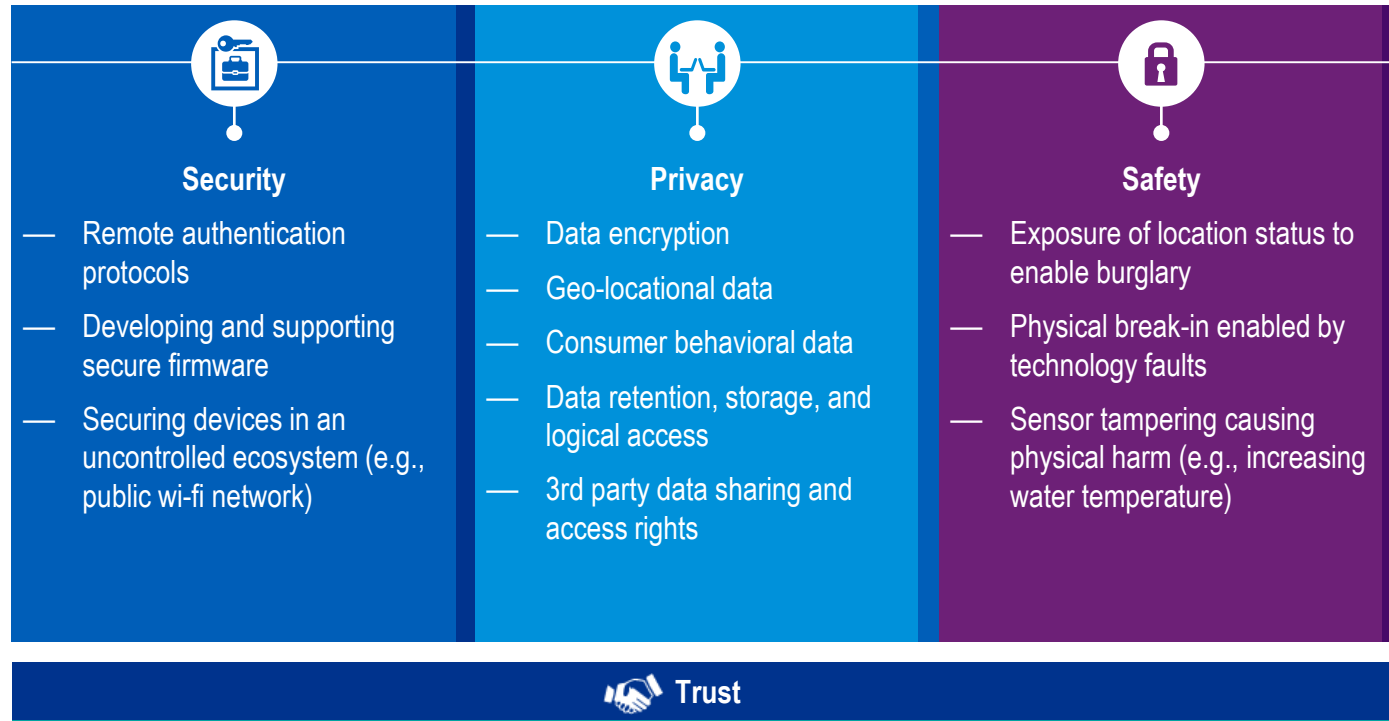**Guy Rosario**
Manager, Cyber Security
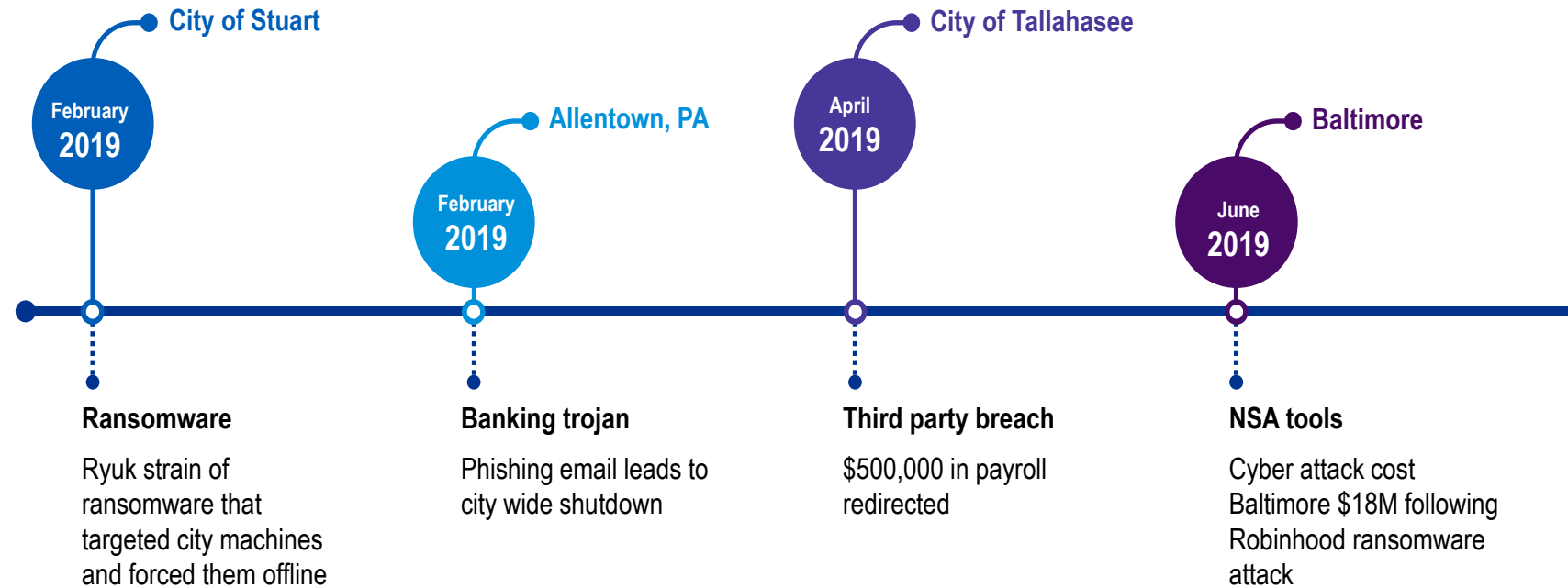T: 250 480 3608
E: grosario@kpmg.ca

Contents

The Challenge

— Significant trends are pressuring and creating the opportunity for, many cities to transform, creating a **moving target for developers, security, and risk professionals**

— The **growing connected ecosystem** introduces new challenges for cities to manage

— IoT has an impact to various risk domains, notably **security, privacy, and safety**, collectively building consumer **trust**

Security
— Remote authentication protocols
— Developing and supporting secure firmware
— Securing devices in an uncontrolled ecosystem (e.g., public wi-fi network)

Privacy
— Data encryption
— Geo-locational data
— Consumer behavioral data
— Data retention, storage, and logical access
— 3rd party data sharing and access rights

Safety
— Exposure of location status to enable burglary
— Physical break-in enabled by technology faults
— Sensor tampering causing physical harm (e.g., increasing water temperature)

Trust

Smart City Opportunity
— Increased connectivity and access
— Enhanced citizen mobility
— Better quality of life
— Improved environmental sustainability
— Better public safety and health
— Stronger economic outcomes

Recent attacks

www.thingful.net
www.shodan.io

City of Stuart

February 2019

Allentown, PA

February 2019

City of Tallahasee

April 2019

Baltimore

June 2019

Ransomware

Ryuk strain of ransomware that targeted city machines and forced them offline

Banking trojan

Phishing email leads to city wide shutdown

Third party breach

$500,000 in payroll redirected

NSA tools

Cyber attack cost Baltimore $18M following Robinhood ransomware attack

Key factors

Inadequate asset management

Increased attack surface

Inadequate security governance

Infrequent security assessment

Lack of security requirements planning

No identification of crown jewels

No response planning, coordination or testing

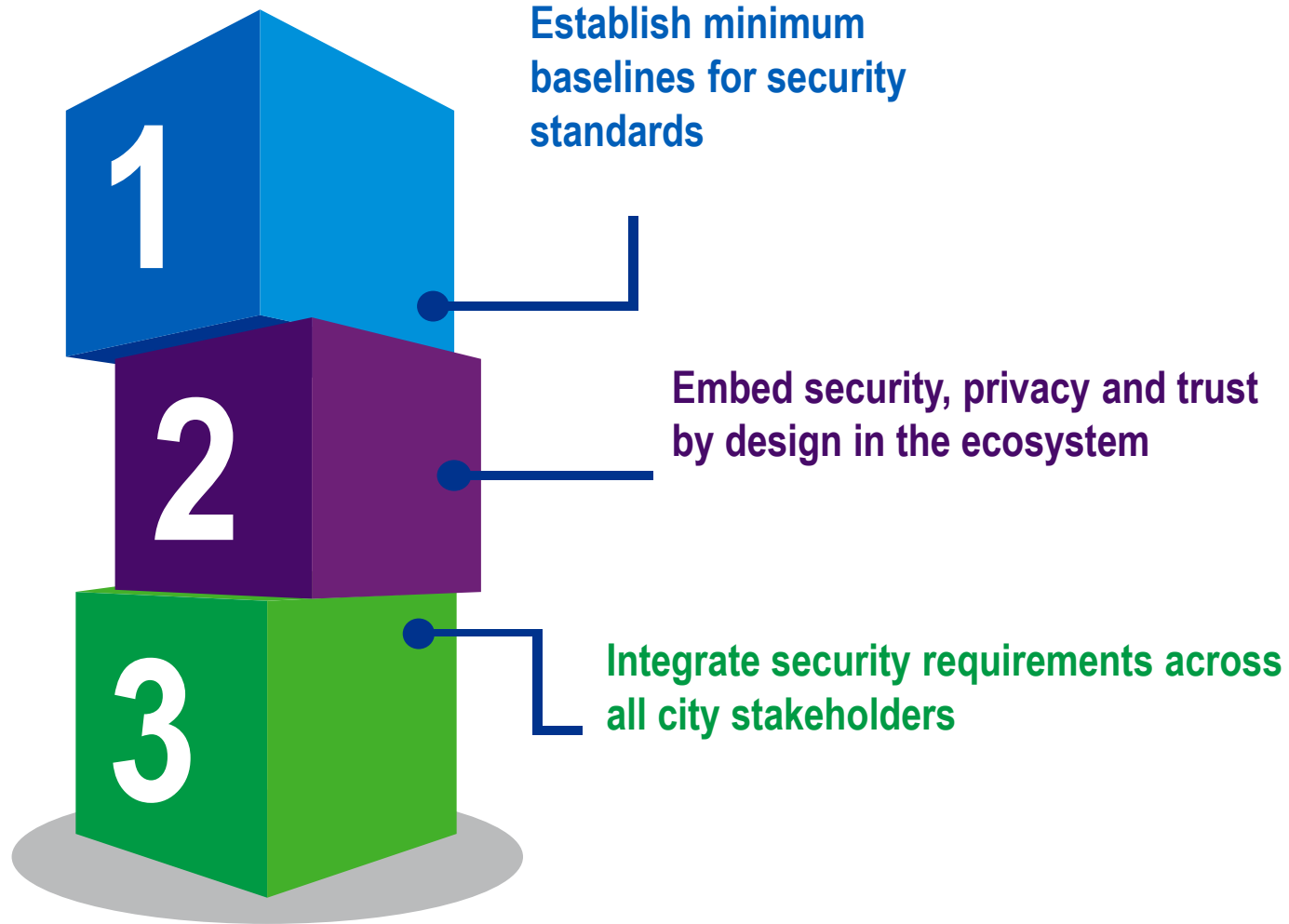Weak monitoring controls

Shadow IT

Legacy systems

Complexity in patch deployment

Inadequate physical security

Lack of encryption

No third party/vendor risk assessment

No collaboration with stakeholders

Building trust

1 — Establish minimum baselines for security standards

2 — Embed security, privacy and trust by design in the ecosystem

3 — Integrate security requirements across all city stakeholders

Takeaways

01 — Baseline Standards
- Secure interoperability
- Secure connection over the web
- Authentication, authorization, cryptography, auditing & alerting, patching, updating, configurations & more

02 — Security, Privacy, Trust by Design
- Secure deployment
- Privacy measures, data protections, rights allocations
- Industry and regulatory needs, policy, compliance, communications

03 — Stakeholder Integration
- Demonstration of capabilities
- Accreditation, audit, assurance
- Collaboration, innovation

Guiding Principles

Inherently secure technology establishes a foundation for a safe, reliable, and confidential consumer experience.

Consumer data is at the heart of public trust and perception and must be properly managed throughout the lifecycle.

A strong principles-based design embedded into product development is cost-effective and operationally preferred.

Data integrity, security, and privacy are key in successful product adoption and deployment.

An effective governance framework helps mitigate financial, operational, compliance, cybersecurity, and reputational risks.

Thank you

Contacts

Jason Stevenson
Director, Cyber Security
T: 250 480 3531
E: jasonstevenson@kpmg.ca

Guy Rosario
Manager, Cyber Security
T: 250 480 3608
E: grosario@kpmg.ca