Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

Jan. 9, 2019

ISOAG Jan 9, 2018 Agenda

I. Welcome & Opening Remarks	Mike Watson, VITA
II. Secure Web Application Development	Chiedo John, Chiedo Company
III. Verizon Data Breach investigations Report	Marc Spitler, Verizon
IV. Interplay of Business, IT and Security	Aaron Mathes, CGI
V. Upcoming Events	Mike Watson
VI. Partnership Update	SAIC

Web Application Security For Project Managers

chiedolabs.com

Hey, I’m Chiedo

I’ve Done Some Cyber

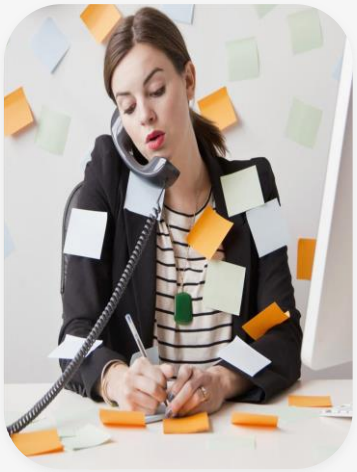
How to Build Secure Web Apps

For Project and
IT Managers

Not for
Developers

The Problem

New Tech is Always Surfacing



IT Managers Become the Default

Without Training and Without Time

This Happens a Lot with Web Tech

Common Issues With Developers

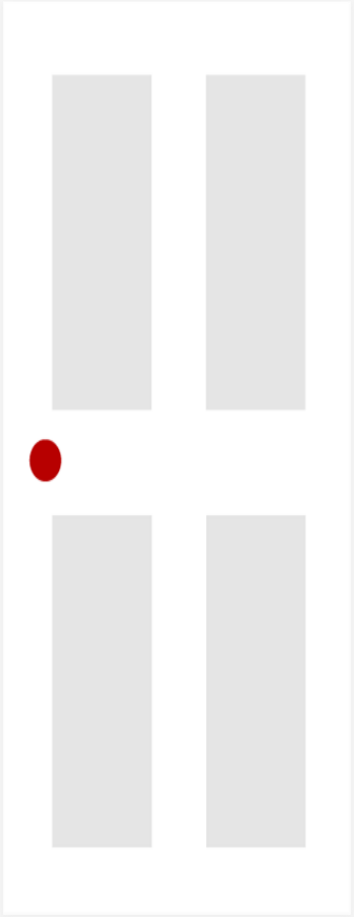
Micro focus rather than a macro focus

Functionality prioritized over security

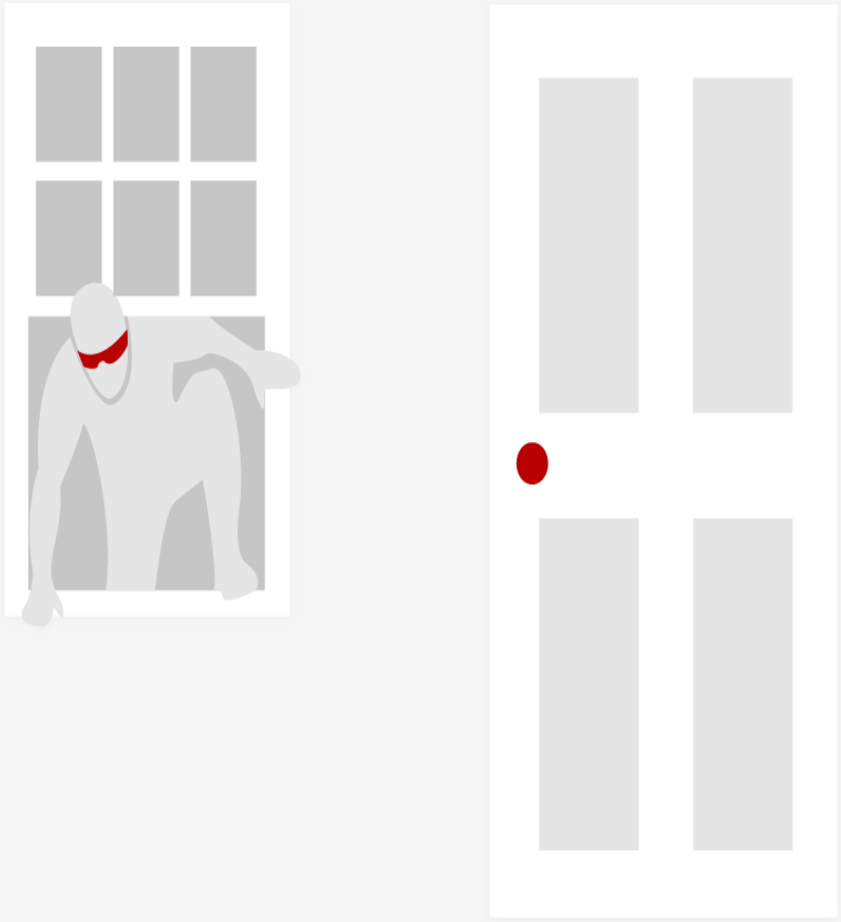
Usually no security training

Lack of ownership. Turnover

What a Developer Sees



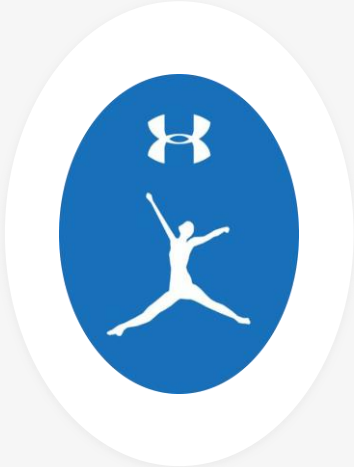
But you need to see Gaps



Gaps are Costly

Facebook
~29M Affected

Quora
~100M Affected



MyFitnessPal
~150M Affected

Marriott
~500M Affected

And Only You Can Prevent Forest Fires

Security Has to Exist at the Top

Let's Talk About Web Security

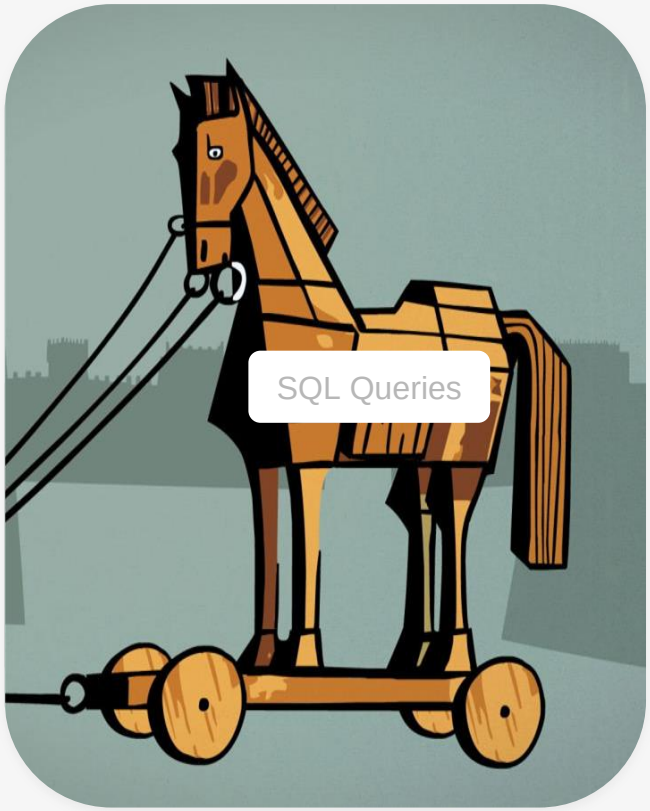
OWASP

OWASP Top 10


2017
OWASP
TOP
10
APPLICATION
SECURITY RISKS
A1
INJECTION
A2
BROKEN AUTHENTICATION
A3
SENSITIVE DATA EXPOSURE
A4
XML EXTERNAL ENTITIES (XXE)
A5
BROKEN ACCESS CONTROL
A6
SECURITY MISCONFIGURATION
A7
CROSS-SITE SCRIPTING (XSS)
A8
INSECURE DESERIALIZATION
A9
USING COMPONENTS WITH KNOWN VULNERABILITIES
A10
INSUFFICIENT LOGGING & MONITORING

See the Forest

1: Injection



Preventions

- Utilize an ORM
- Prepare all SQL statements
- User Input Validation

2: Broken Authentication

Preventions

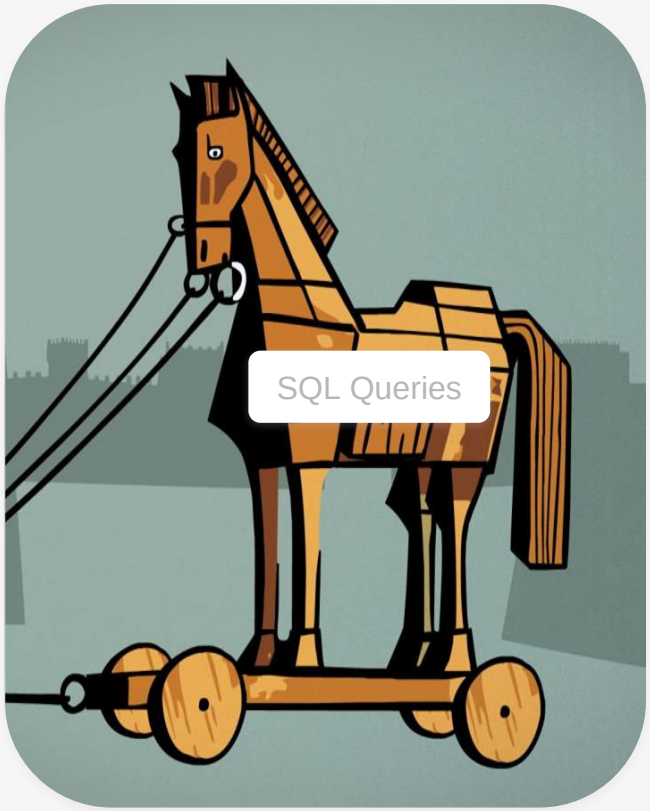
- Understand the Authentication Scheme Being Used
- Write and Maintain Automated Unit Tests

3: Sensitive Data Exposure

Preventions / Mitigations (hard)

- Encrypt Sensitive Data Appropriately (In-transit and/or at-rest)
- Document Your Sensitive Assets and Their Touch Points
- Limit Third-party Access to Sensitive Data

4: XML External Entities (XME)



Preventions

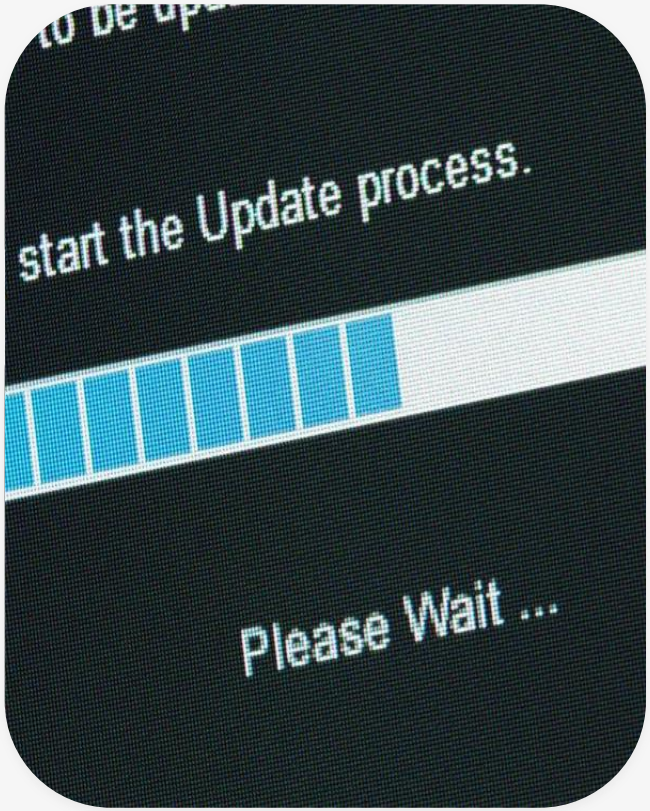
- Utilize an XML Parser with Secure Defaults
- Disable DTDs (External Entities) completely

5: Broken Access Control

Preventions

- Write and Maintain Access Control Documentation
- Write and Maintain Automated Unit Tests
- Hire a Pen Tester to Continually Assess Security

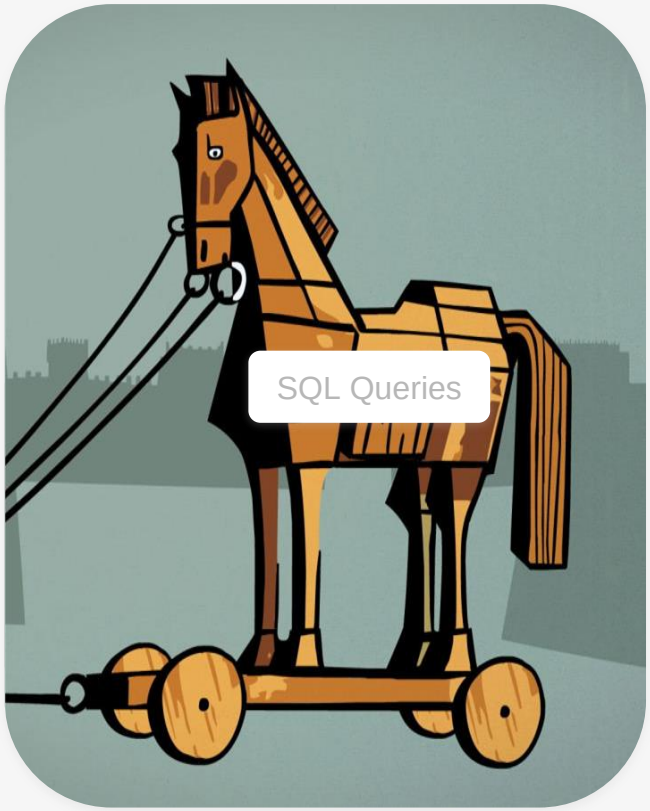
6: Security Misconfiguration



Preventions (hard)

- Create Update Schedules For Software & Languages
- Change Default Passwords
- Ensure Error Handling is Private on Production
- Set Secure Defaults for All Libraries
- Review Third-Party Security Configs (S3, DNS, etc)

7: Cross-site Scripting (XSS)



Preventions

- Utilize Templating Libraries with Sane Defaults.
- User Input Validation
- Default to Not Outputting Untrusted Data
- Escape All “Whitelisted” Untrusted Data

8: Insecure Deserialization

Preventions

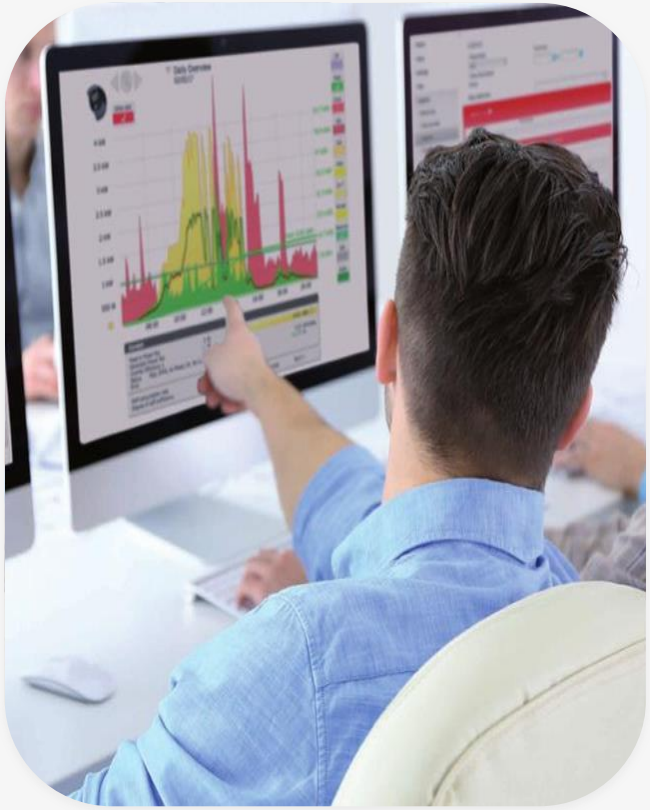
- Authenticate (Sign) All Serialized Objects
- Use JSON Rather than Native (de)serialization Formats. Abstract Away.

9: Components With Known Vulnerabilities

Preventions

- Create Update Schedules For All Packages
- Use Tools That Check For Known Vulnerabilities
- Remove Components That Fail To Fix Vulnerabilities

10: Insufficient Logging and Monitoring



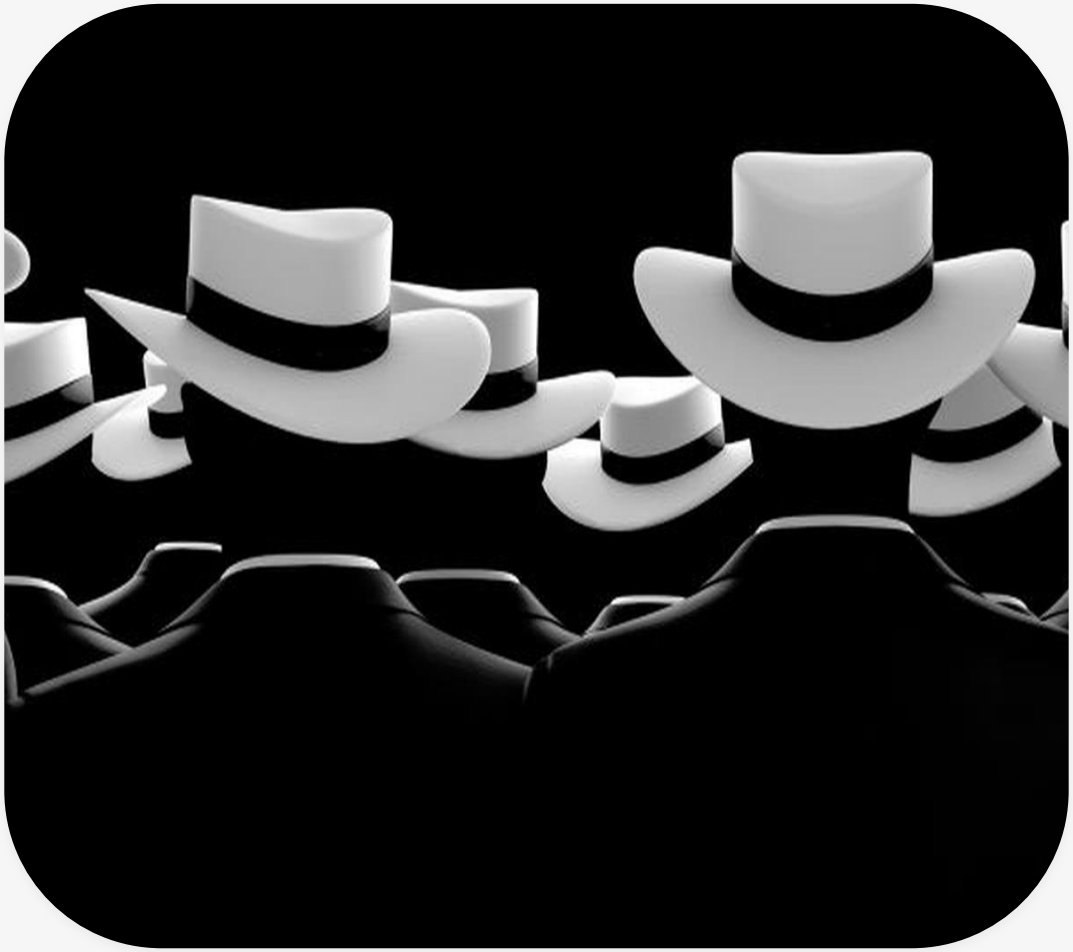
Preventions

- Use Third-Party Software and AI to Monitor logs for Anomalies
- Ensure Developers Log Important Transactions, Log-in Attempts, etc.
- Ensure Logs Supply Adequate Context Without Leaking Sensitive Data.

Lightning Round: Common Mistakes

No HTTPS	Passwords in Plain Text	No Automated Tests	Improper Secret Management
Staging Servers With Live Data	AWS Misconfigurations	No Two-Factor Authentication	Weak Passwords
Out-of Date Software	No Developer Redundancy	Stack Overflow Abuse	Poor Access Control

Hire Help

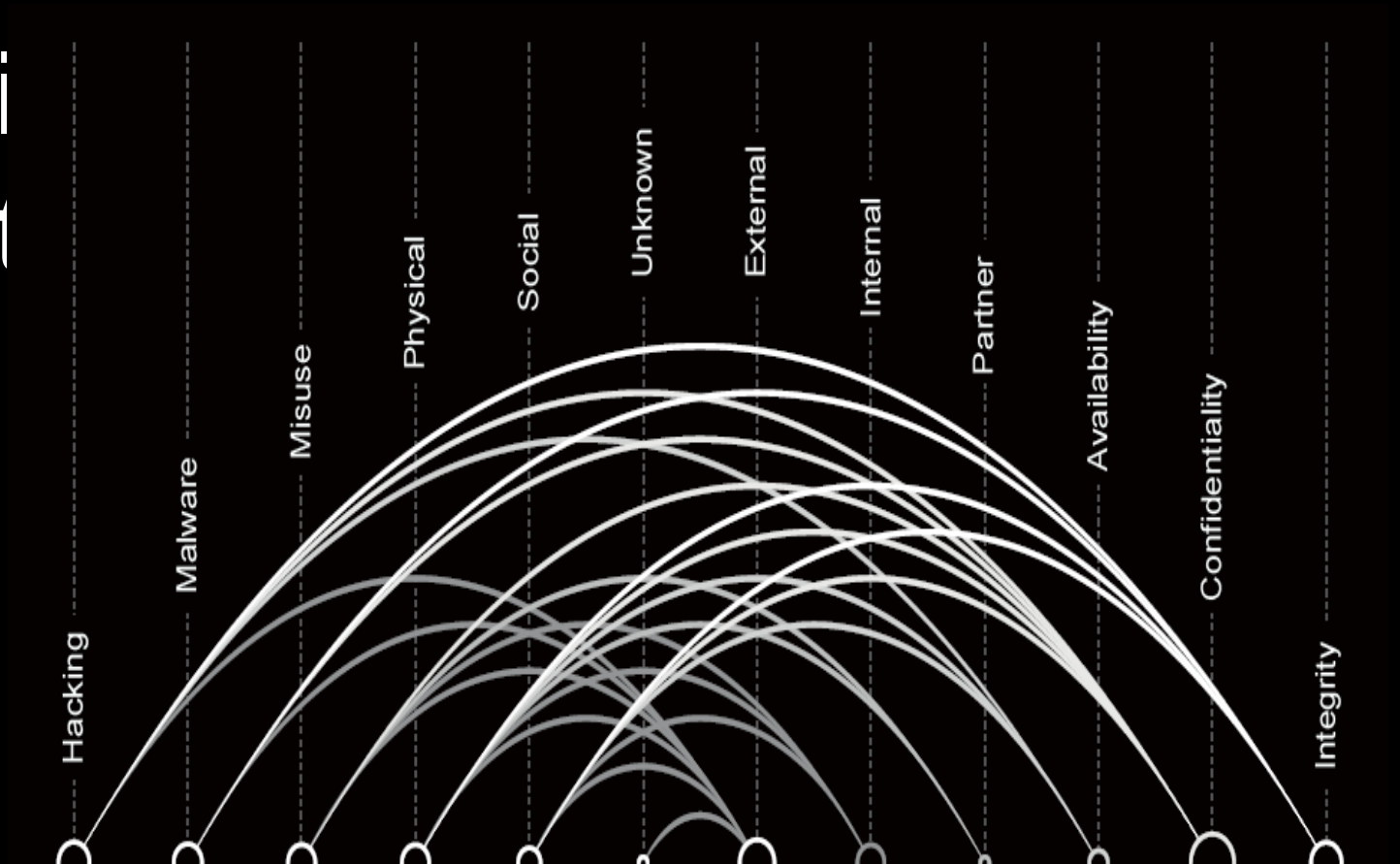


But It's Your Responsibility

Questions?

chiedolabs.com

Cybercrime trends 2018 Verizon Data Breach Investi Report



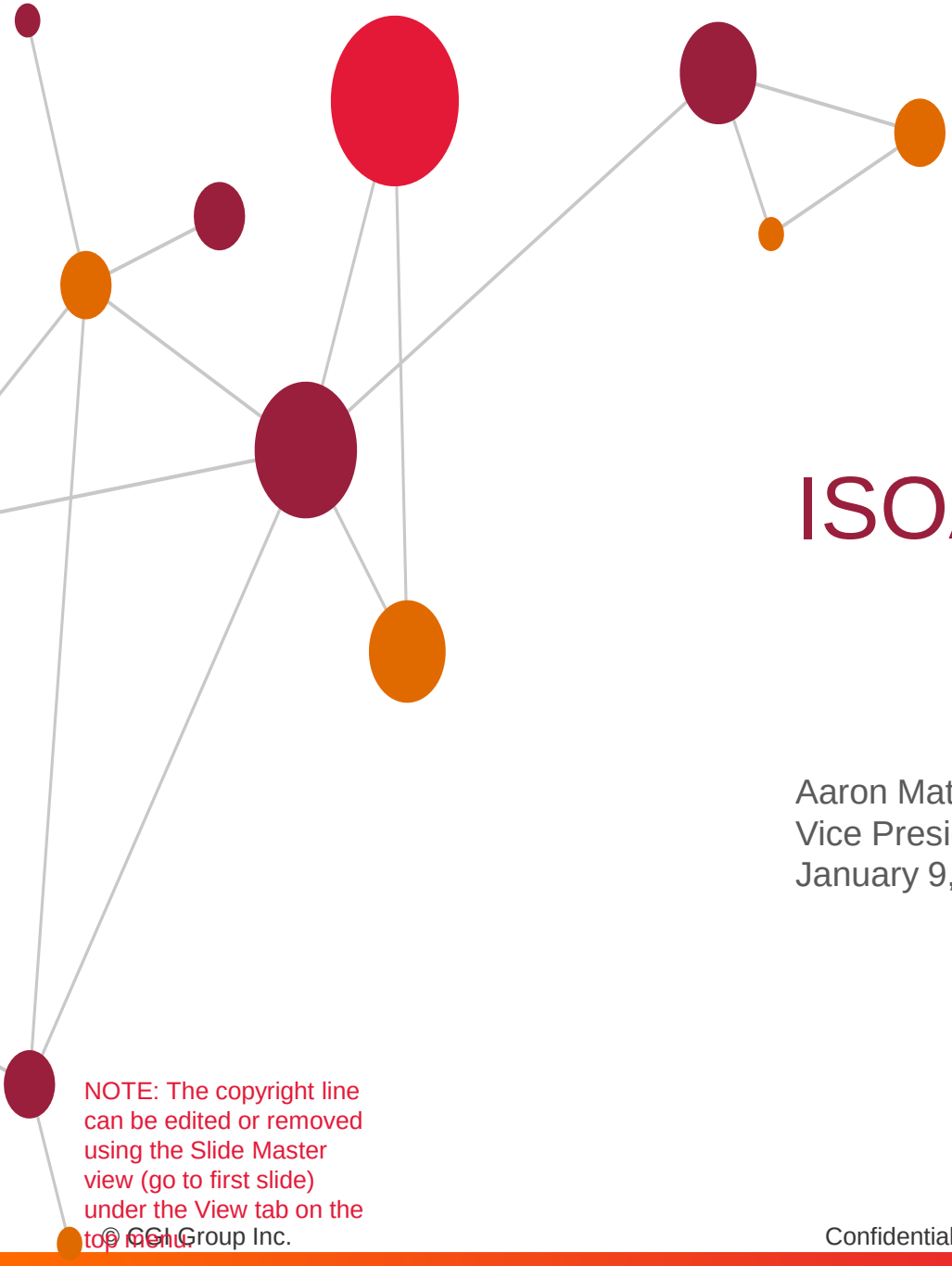
verizon

Proprietary statement

***This presentation is not being shared publically**

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

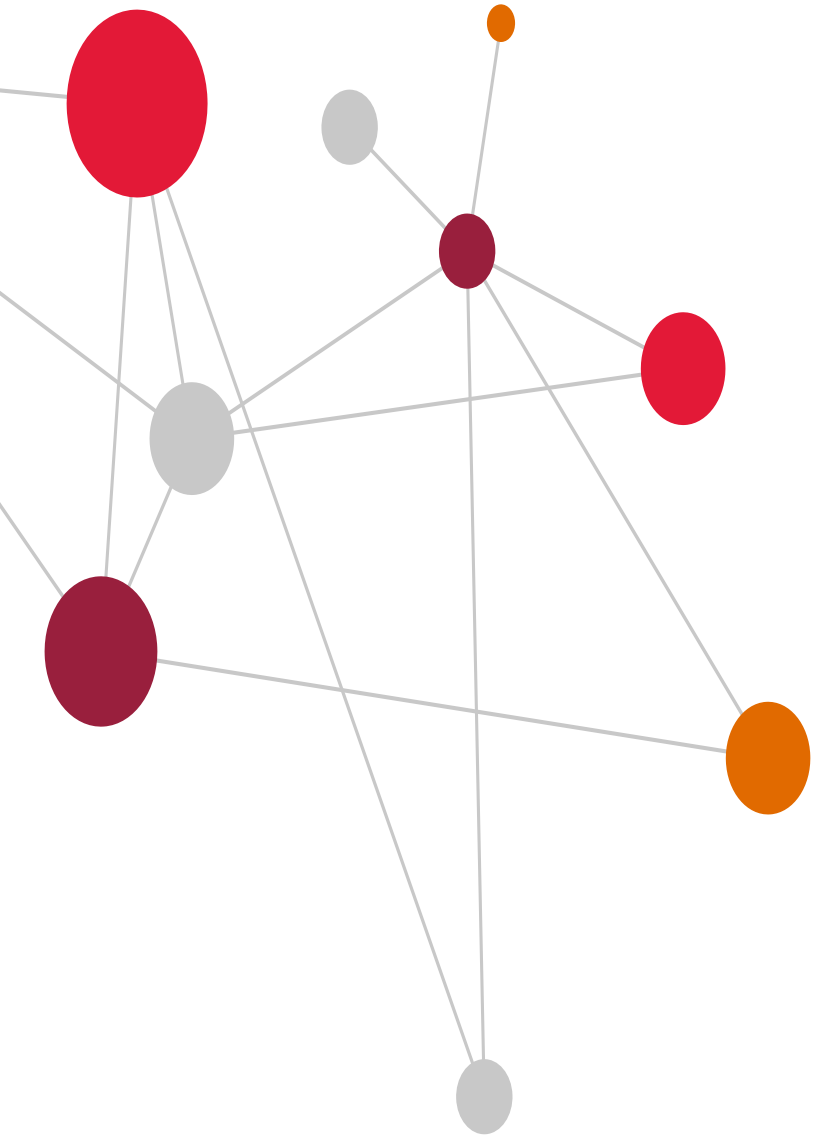


Experience the commitment®

ISOAG

Aaron Mathes
Vice President, Sector Lead
January 9, 2019

NOTE: The copyright line can be edited or removed using the Slide Master view (go to first slide) under the View tab on the top menu.



Experience the commitment®

Discussion of the Interplay of Business, IT and Security

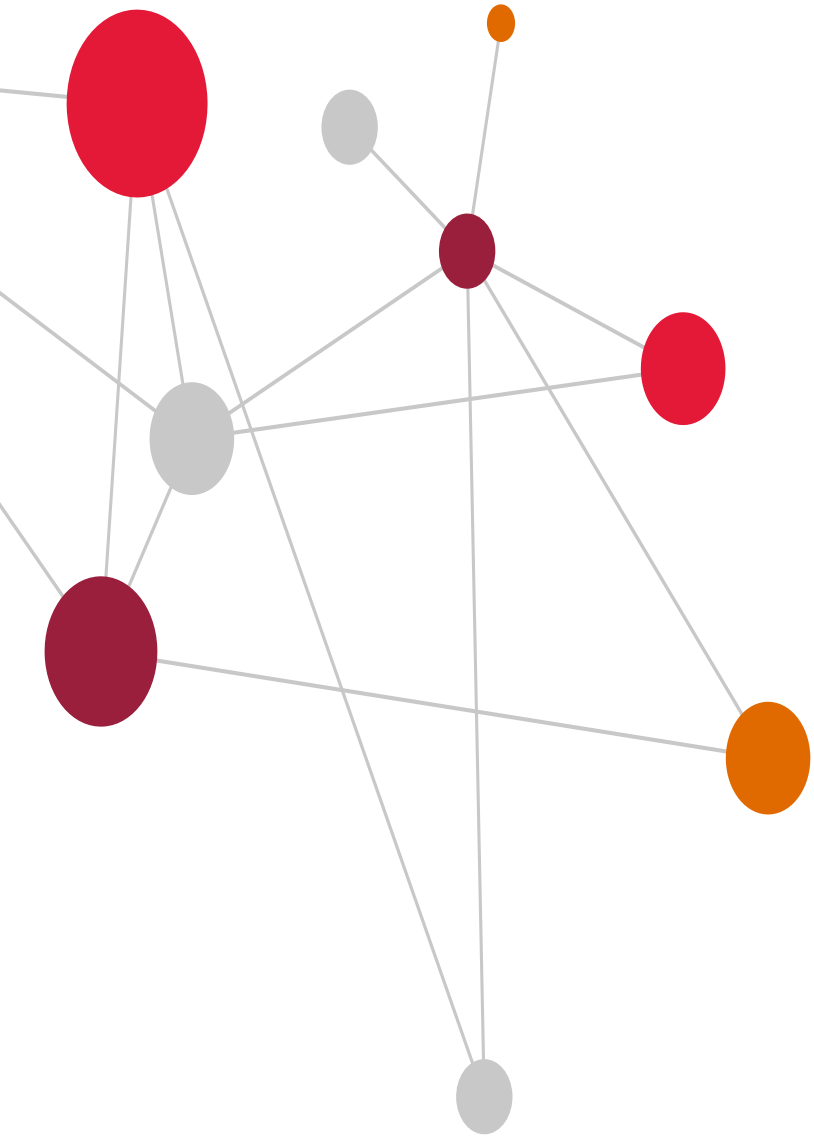
Introduction

Aaron Mathes
VP, Consulting Services
US Mid-Atlantic Sector Lead

Aaron serves with a world class team focused on CGI's commercial and public sector clients across the Mid-Atlantic States. He also serves on several boards including director on the Virginia Chamber of Commerce, Chesterfield County Committee on the Future and the Liberty University School of Engineering and Computational Sciences, Board of Advisors.

Prior to joining CGI, Aaron M. Mathes served as Deputy Secretary of Technology for Governor McDonnell in the Commonwealth of Virginia. In this capacity, Mathes oversaw workplace productivity and efficiency solutions based on CRM technology, BYOD, cyber-threat preparedness, government transparency and citizen services. His projects included, supporting technology related economic development efforts in the areas of innovation, entrepreneurship and the growth of the datacenter footprint in the Commonwealth. In this deputy cabinet role Aaron also acted in a role of overseeing the Virginia Information Technologies Agency (VITA).

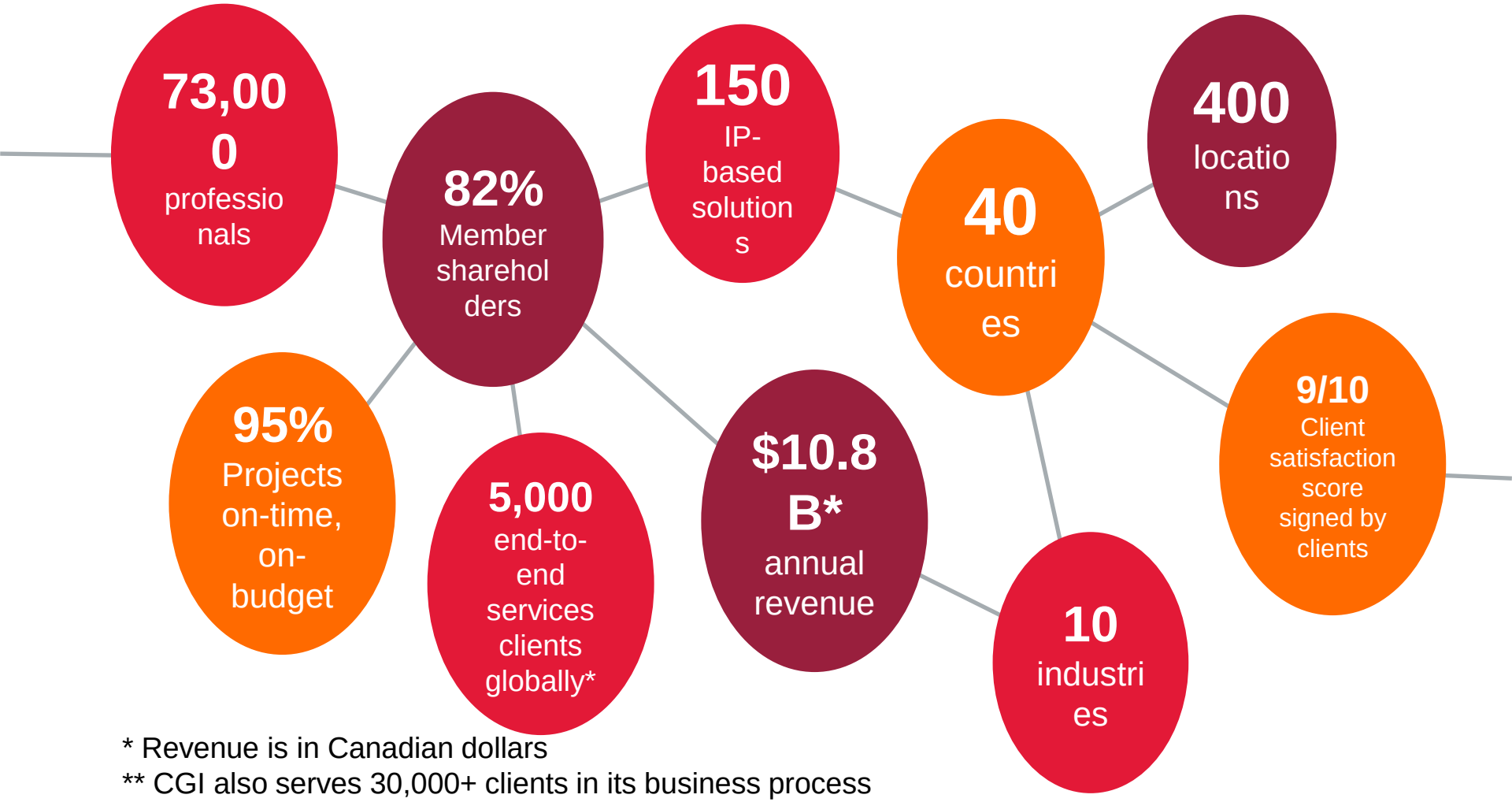
Prior to his service to the Governor, Mathes served as CIO and Information Security Officer for the Virginia Office of Attorney General. Aaron has also held several operational and senior information technology leadership positions at Liberty University including interim CIO, Deputy CIO, with experience that totals more than 20 years in IT management and leadership.



Experience the commitment®

Introduction of CGI

Founded in 1976, CGI is the 5th largest independent end-to-end IT and business consulting services firm in the world

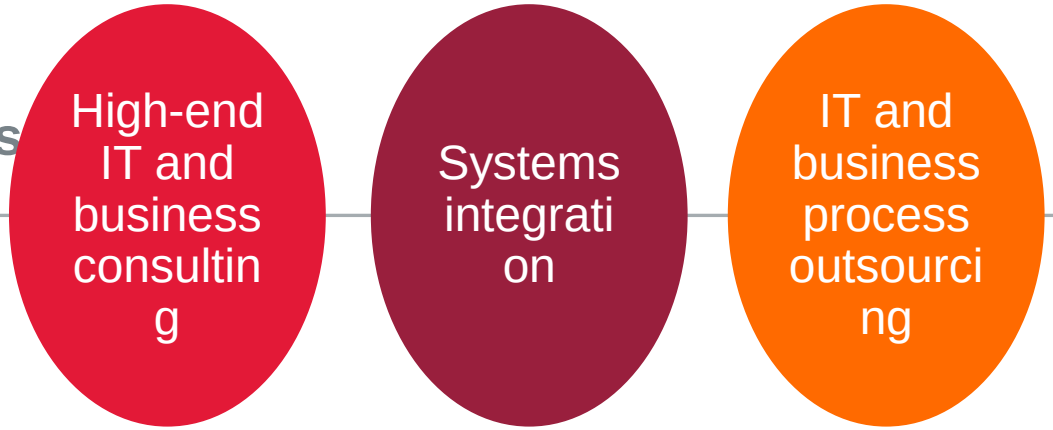


* Revenue is in Canadian dollars

** CGI also serves 30,000+ clients in its business process services operations

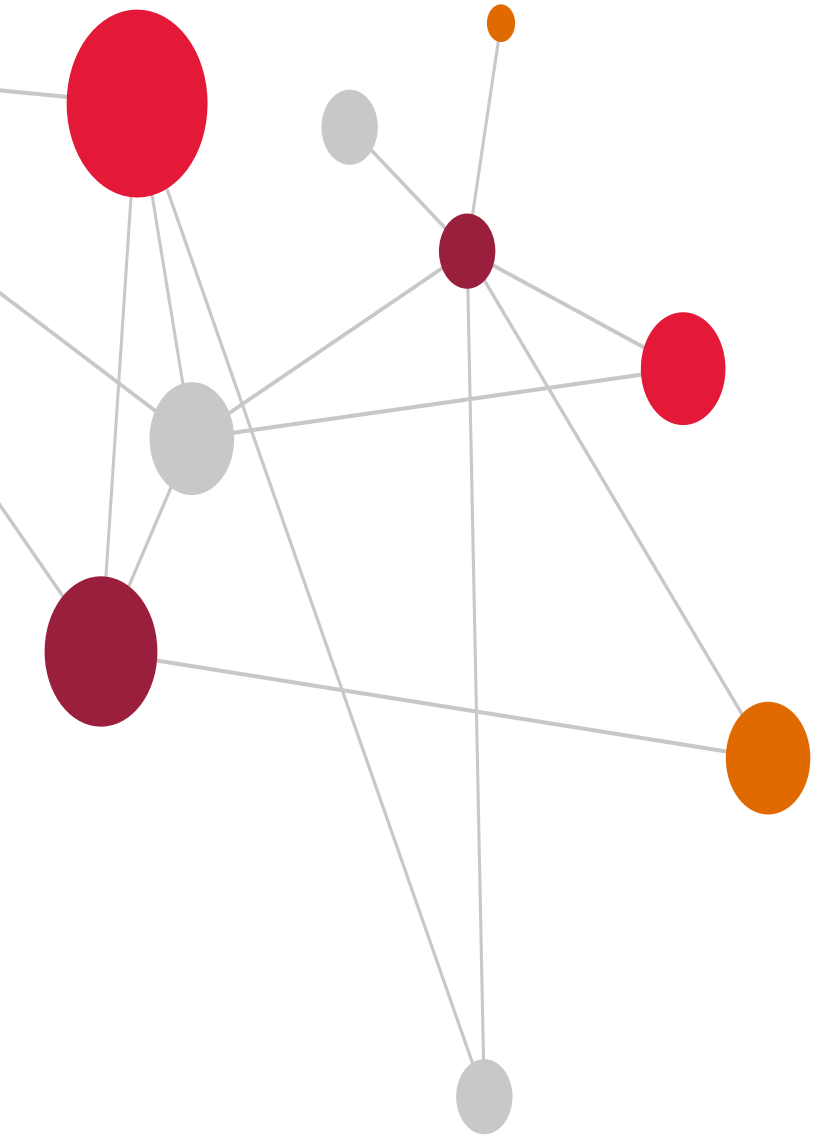
Our range of services and differentiators

Range of services



Differentiators

- **Client-proximity model**
- **Domain expertise**
- **Intellectual Property**
- **Global delivery network**



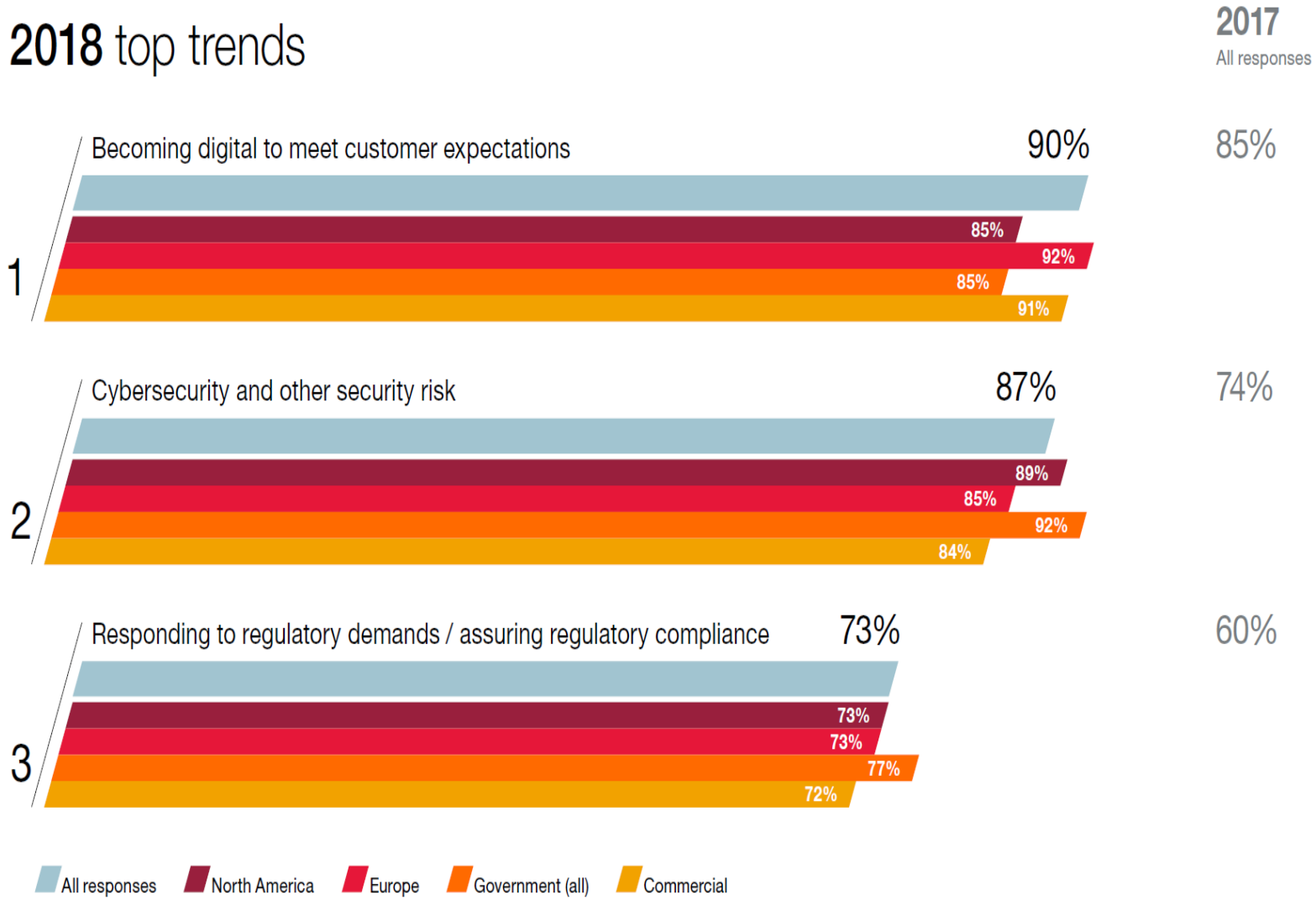
Experience the commitment®

CGI Clients Global Insights and Benchmarking

INTERVIEW INFORMATION: ALL INDUSTRIES

CGI

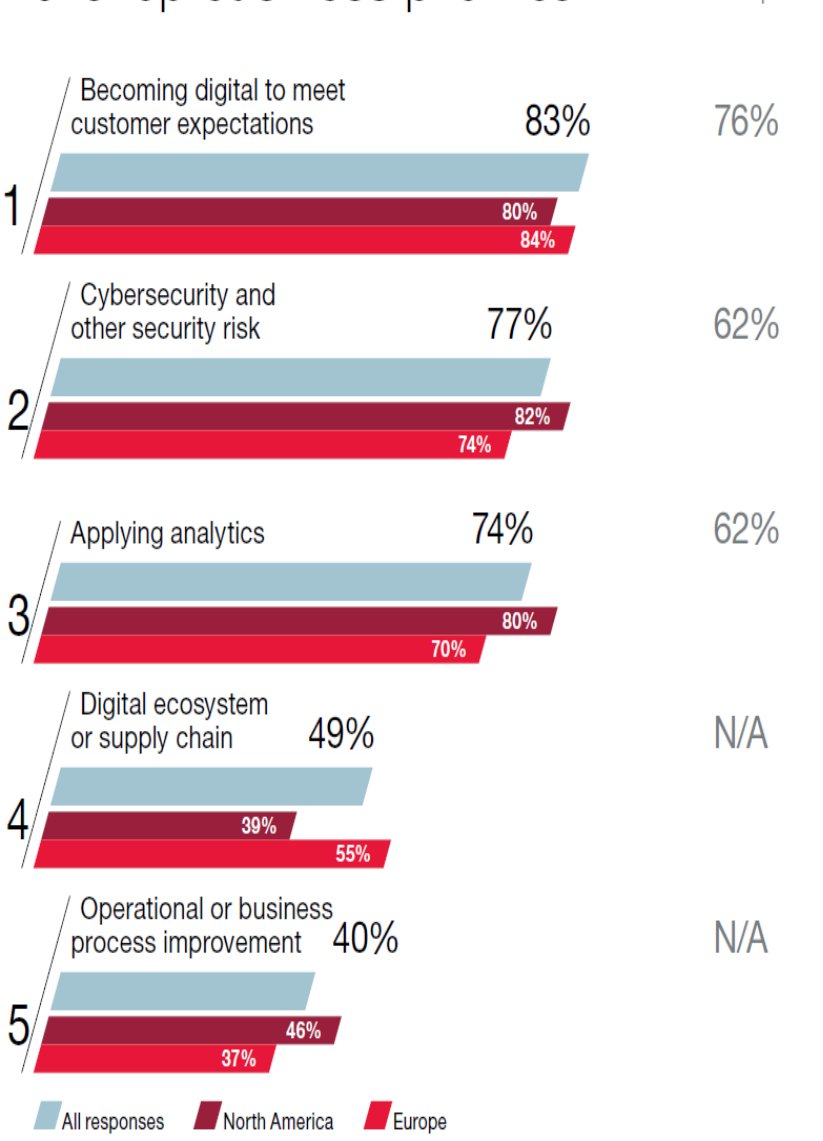
1,434 executives interviewed in 1,000+ organizations across the globe



BUSINESS PRIORITIES

Becoming digital elevates cybersecurity as a top priority

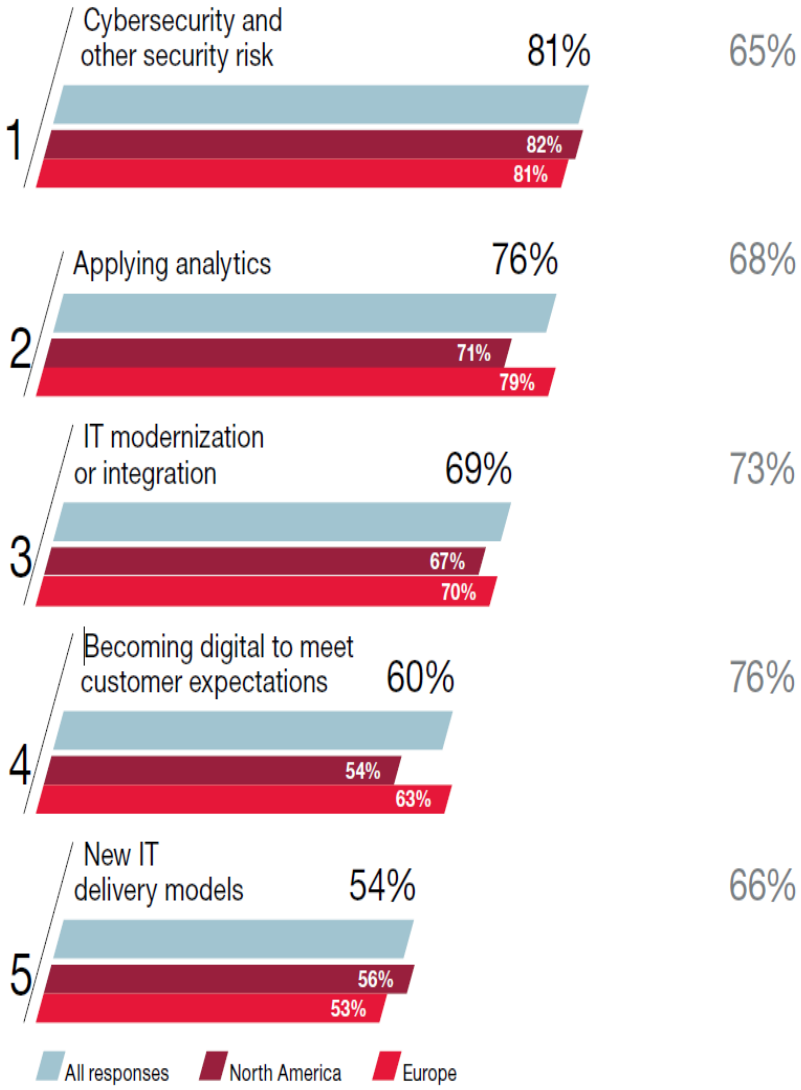
While the top business priority across industries is once again to become digital to meet customer expectations, attention to security risk strengthens as the second most mentioned business priority (up 15%), and now is the top IT priority, reflecting the strong link between digital transformation and protecting the organization.



IT PRIORITIES

Cybersecurity and data privacy

In 2018, cybersecurity and regulation figure prominently among business and IT priorities, increasing in frequency across all industries. Globally, 75% of executives interviewed are focusing on employee training and awareness as the most common response in this area, followed by identifying critical assets for management and control (66%), and testing and verifying cyber response capabilities (64%).



BUSINESS AND IT **PRIORITIES**

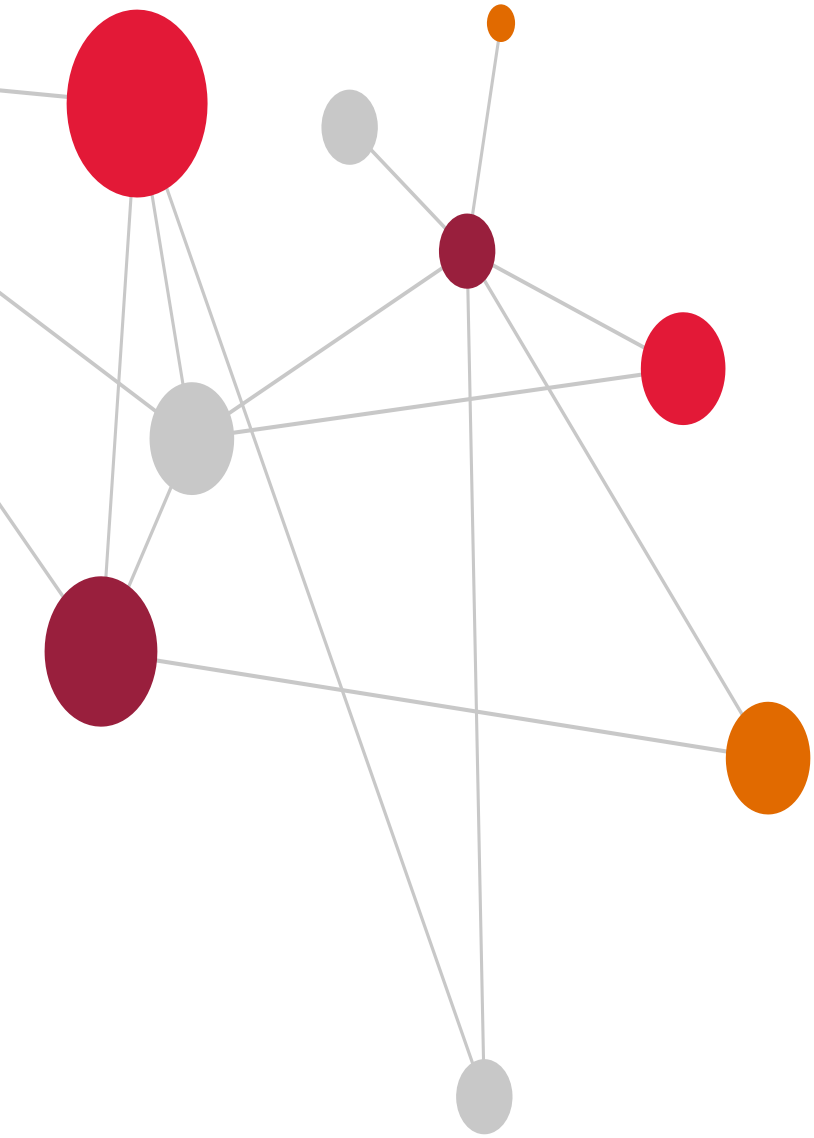
Improving the customer experience while protecting data and systems

As business priorities continue to reflect a focus on the customer and citizen, executives seek to create differentiated, seamless customer experiences to meet rising expectations. Understanding customer interactions and behaviors is critical to improving services, personalizing experiences and driving new business.

Data plays a critical role in helping organizations become more relevant to customers and citizens. Organizations will leverage advanced analytics more broadly to unlock the value of their own data to gain powerful insights into the customer experience, and develop value-added products and services.

At the same time, as organizations seek to use more emerging technologies such as intelligent automation to enhance the customer experience and improve operational efficiency, the "digital drag" of legacy IT continues to hinder progress, keeping modernization a top IT priority.

The business and IT priorities of executives we interviewed are equally focused on protecting data and systems. The threat of security breaches will become even more pronounced as digital transformation continues and vulnerabilities extend beyond the traditional boundaries of the organization. As a result, the digital ecosystem of partners becomes increasingly important as a business priority.

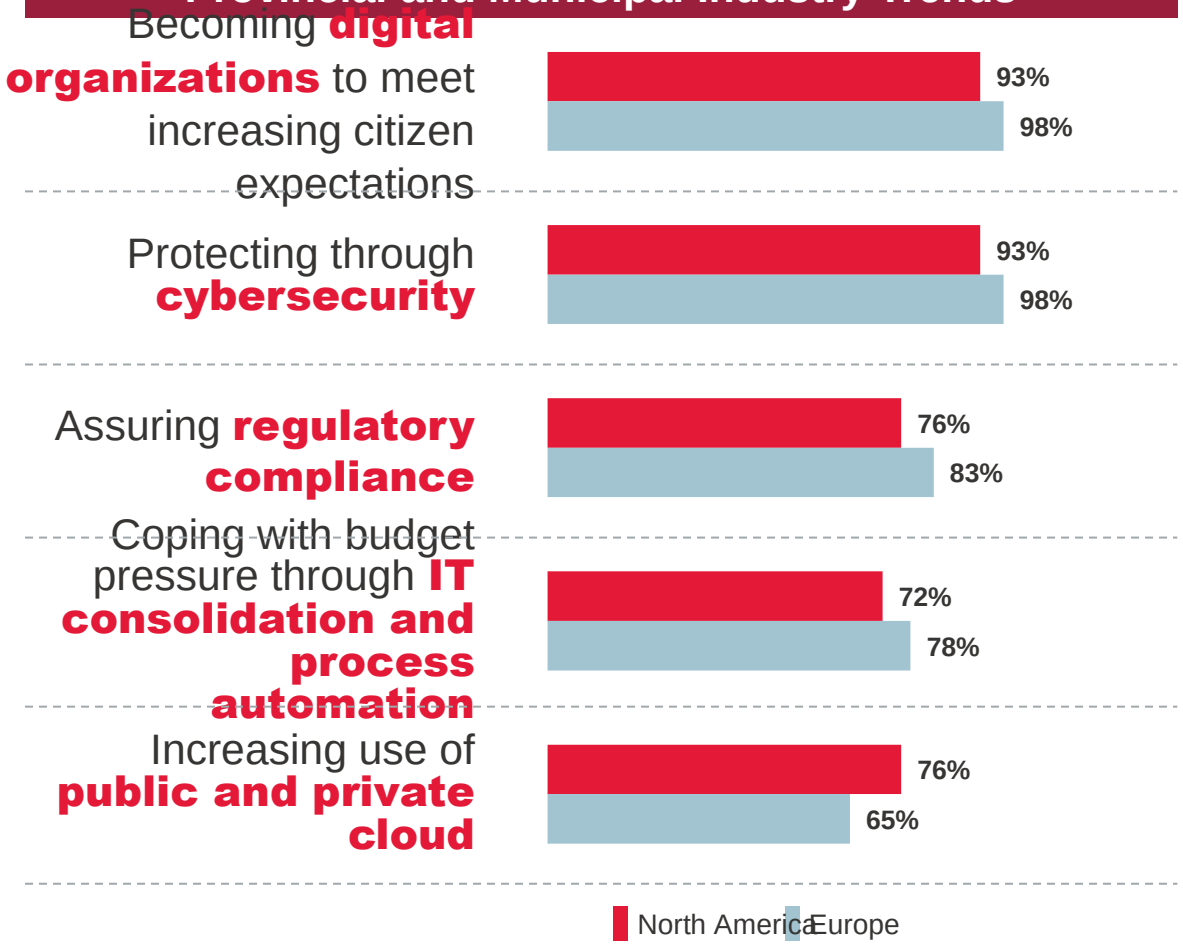


Experience the commitment®

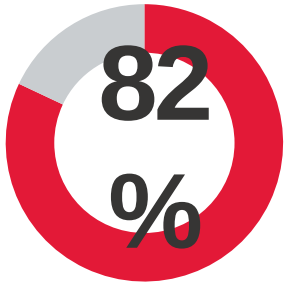
CGI Provincial and Municipal Government Clients Insights and benchmarking

Industry trends: Transforming citizen digital experience; integrating cybersecurity as mission-critical

Provincial and Municipal Industry Trends



Where are you planning to invest in innovation over the next 3 years?



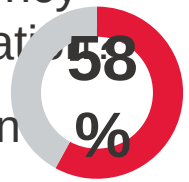
Provinces and municipals across the globe listed **Implementing citizen-facing multi-channel services and engagement** as the top area of investment in the next 3

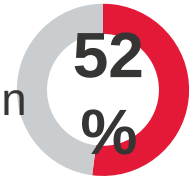
Business priorities: Improve citizen service experience while protecting information; leverage data and analytics to improve outcomes, services

Provincial and Municipal Business Priorities

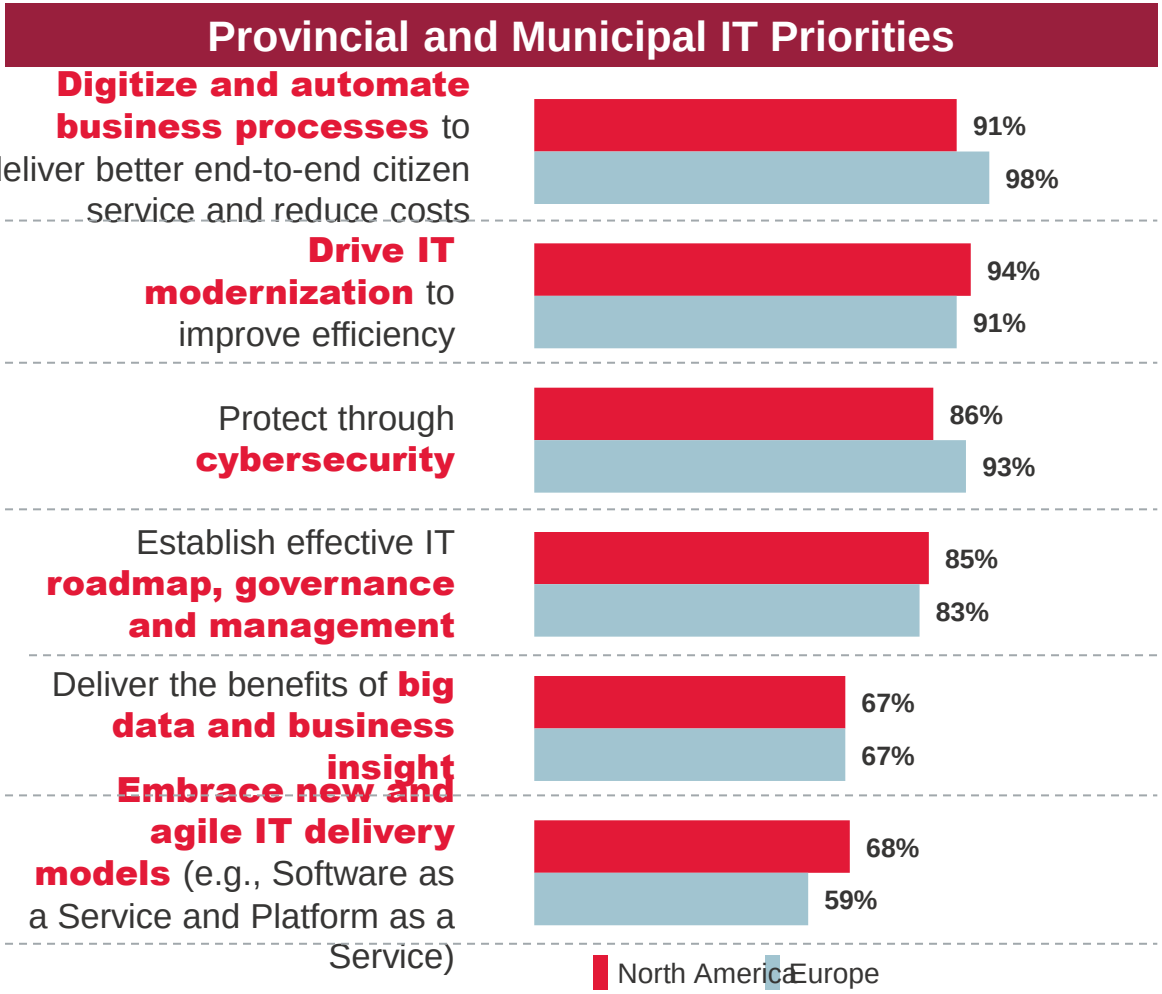
Innovation Investments

What is your priority for Facilitating Cross-agency Collaborati

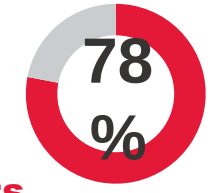




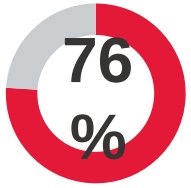
IT priorities: Process automation, modernization and security in focus for improving citizen services

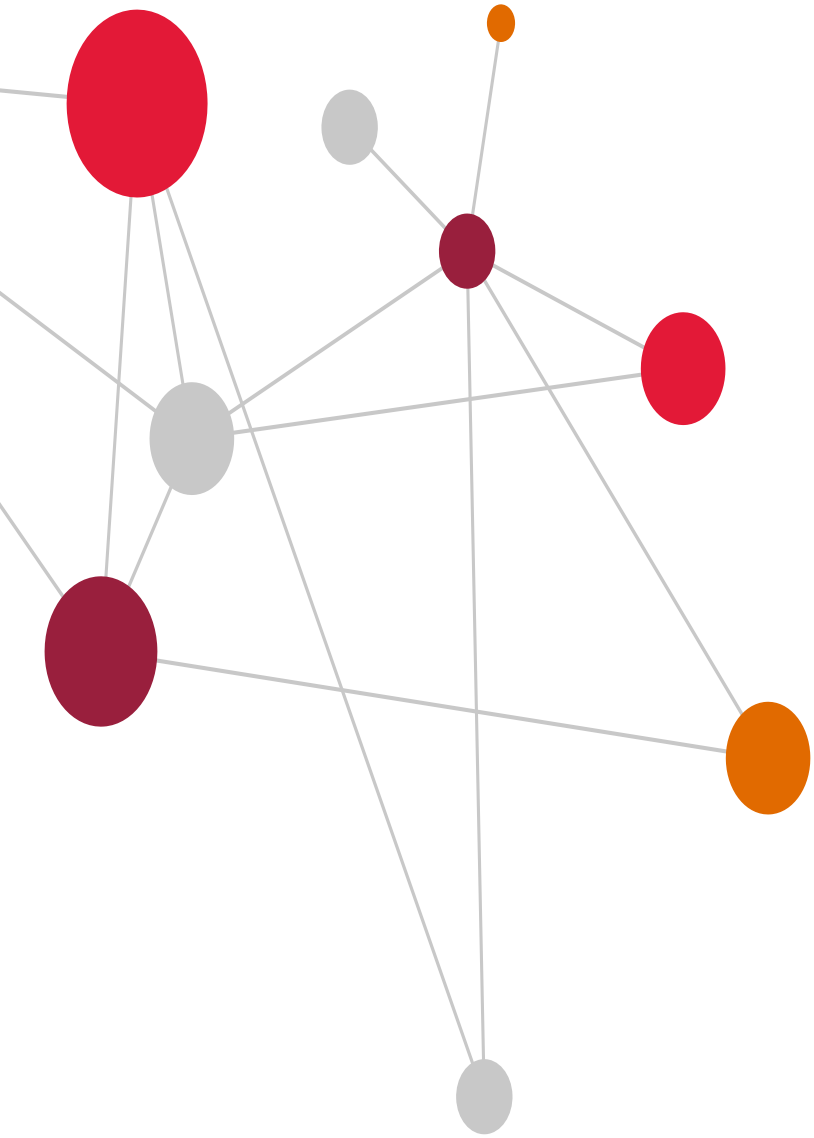


Indicated **Enabling business process improvements** is driving IT spending trends globally



Indicated **Implementing citizen-facing multi-channel services and engagement** is a top area of investment for innovation

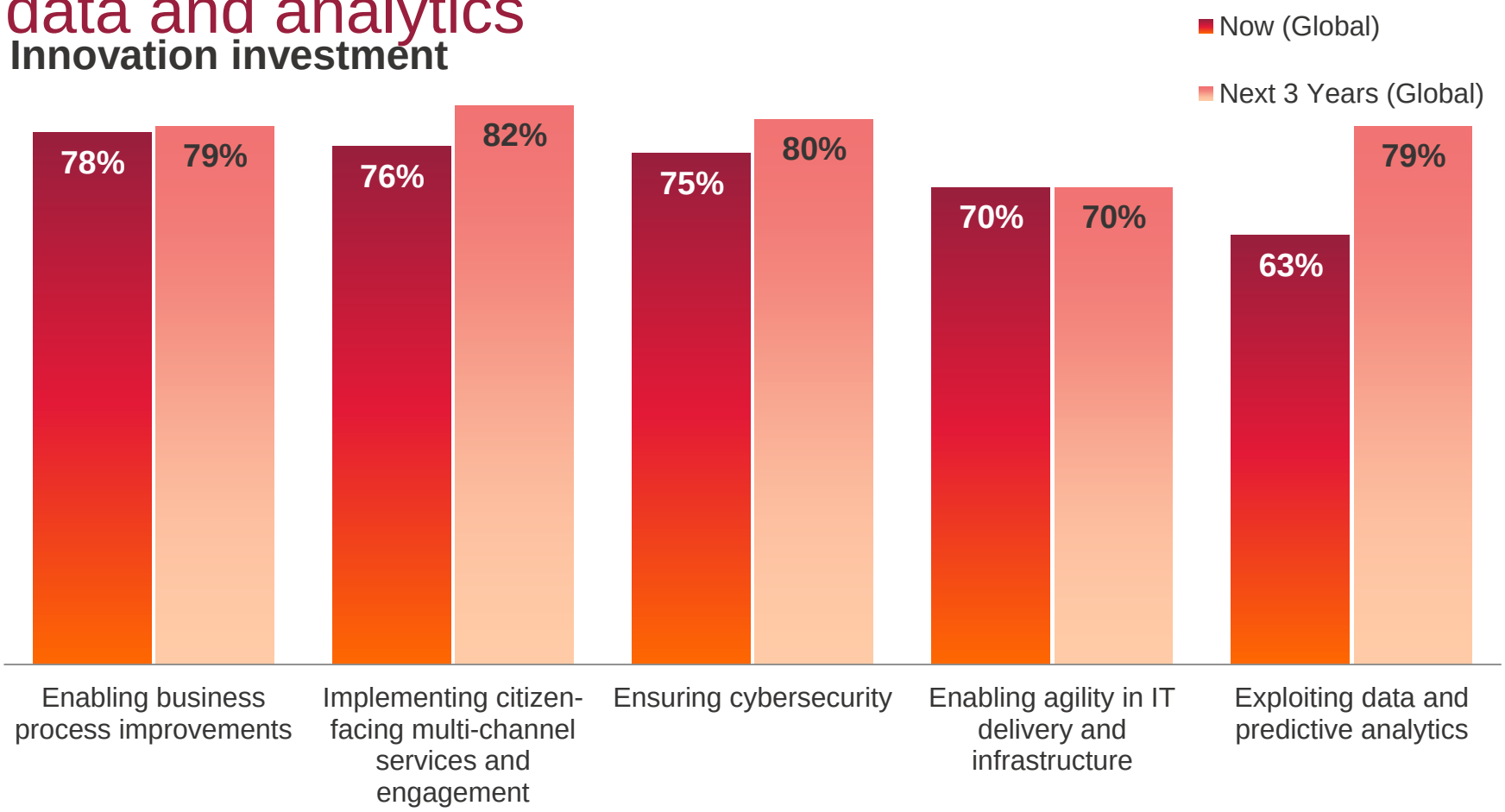




Services and Solutions of Key Interest in Provincial and Municipal Government

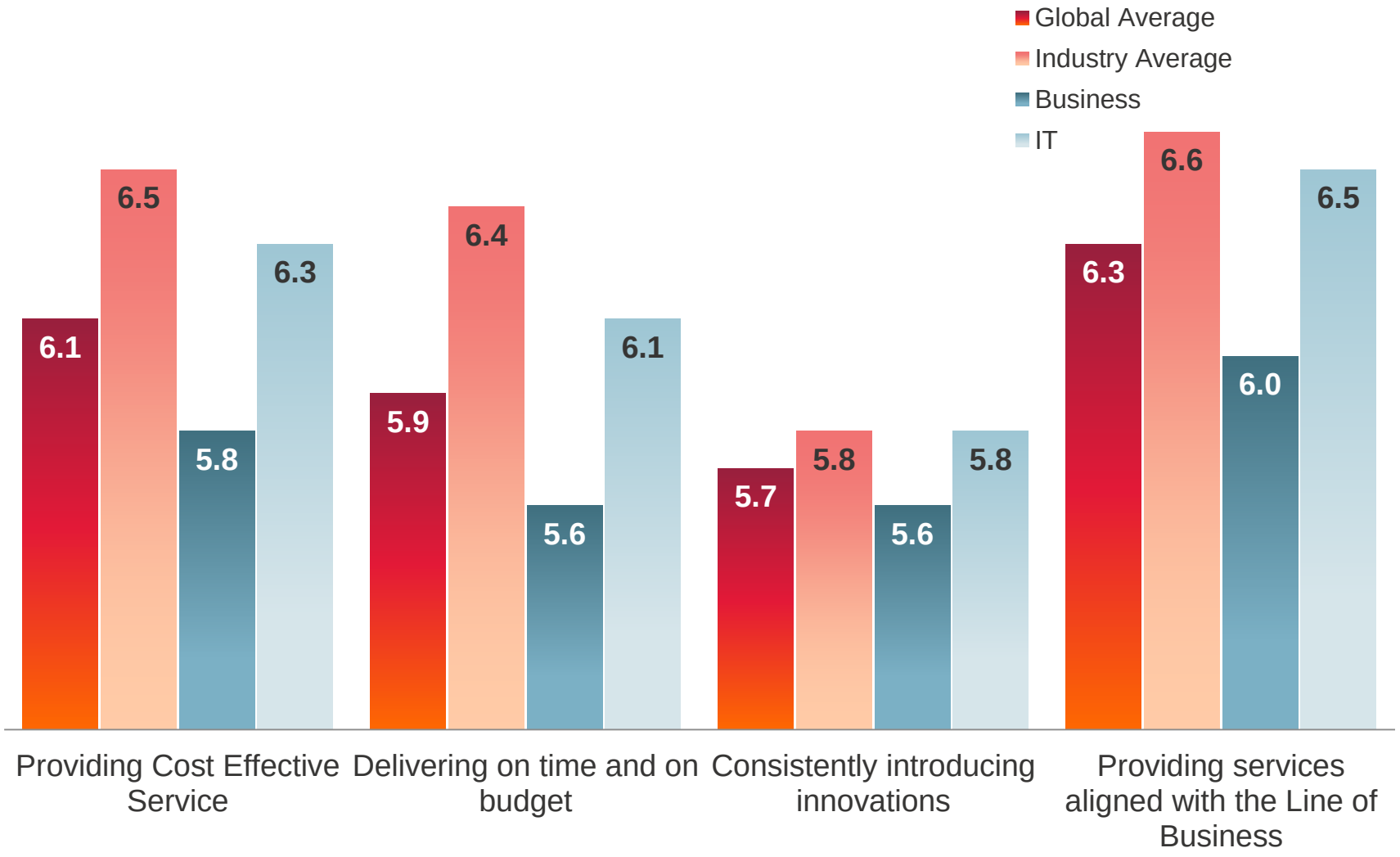
Experience the commitment®

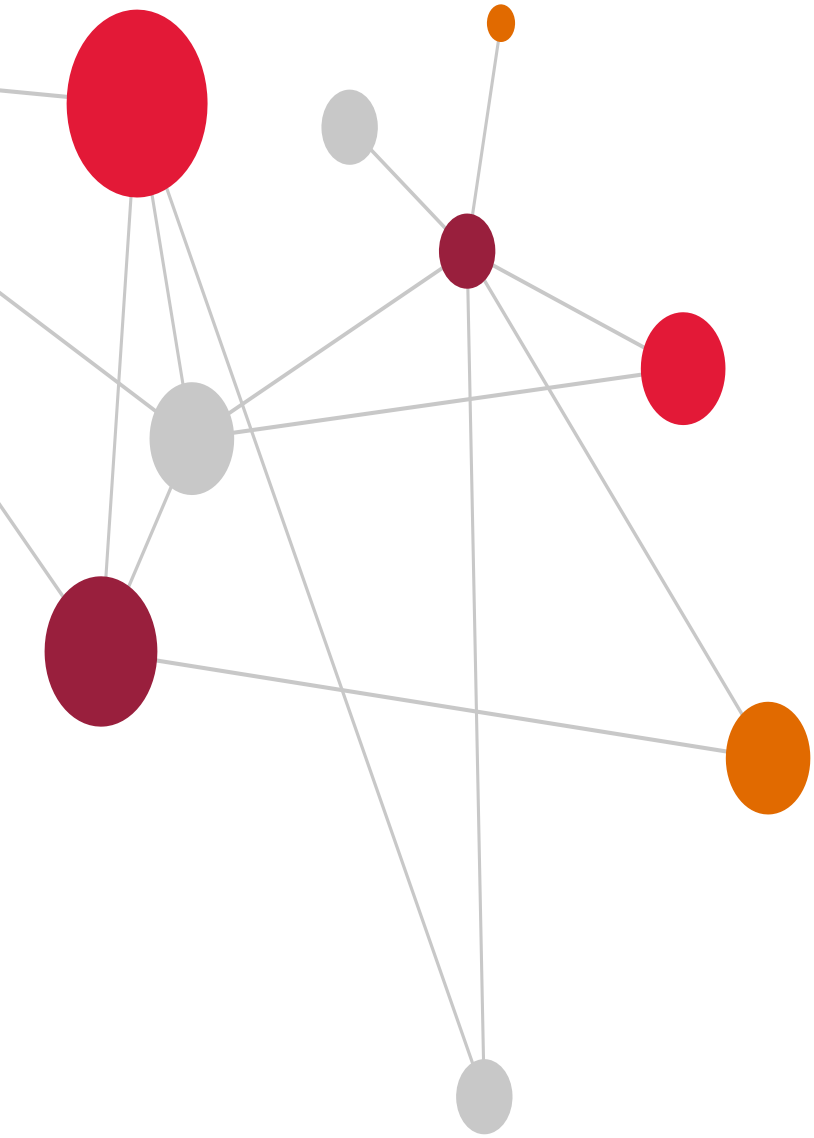
Innovation investment: Focused on implementing citizen-facing multi-channel services, ensuring cybersecurity and exploiting data and analytics



IT Satisfaction: Opportunities to improve alignment between the business and IT organizations

Business Satisfaction vs. IT Satisfaction (Scores from 1 to 10, with 10 most satis

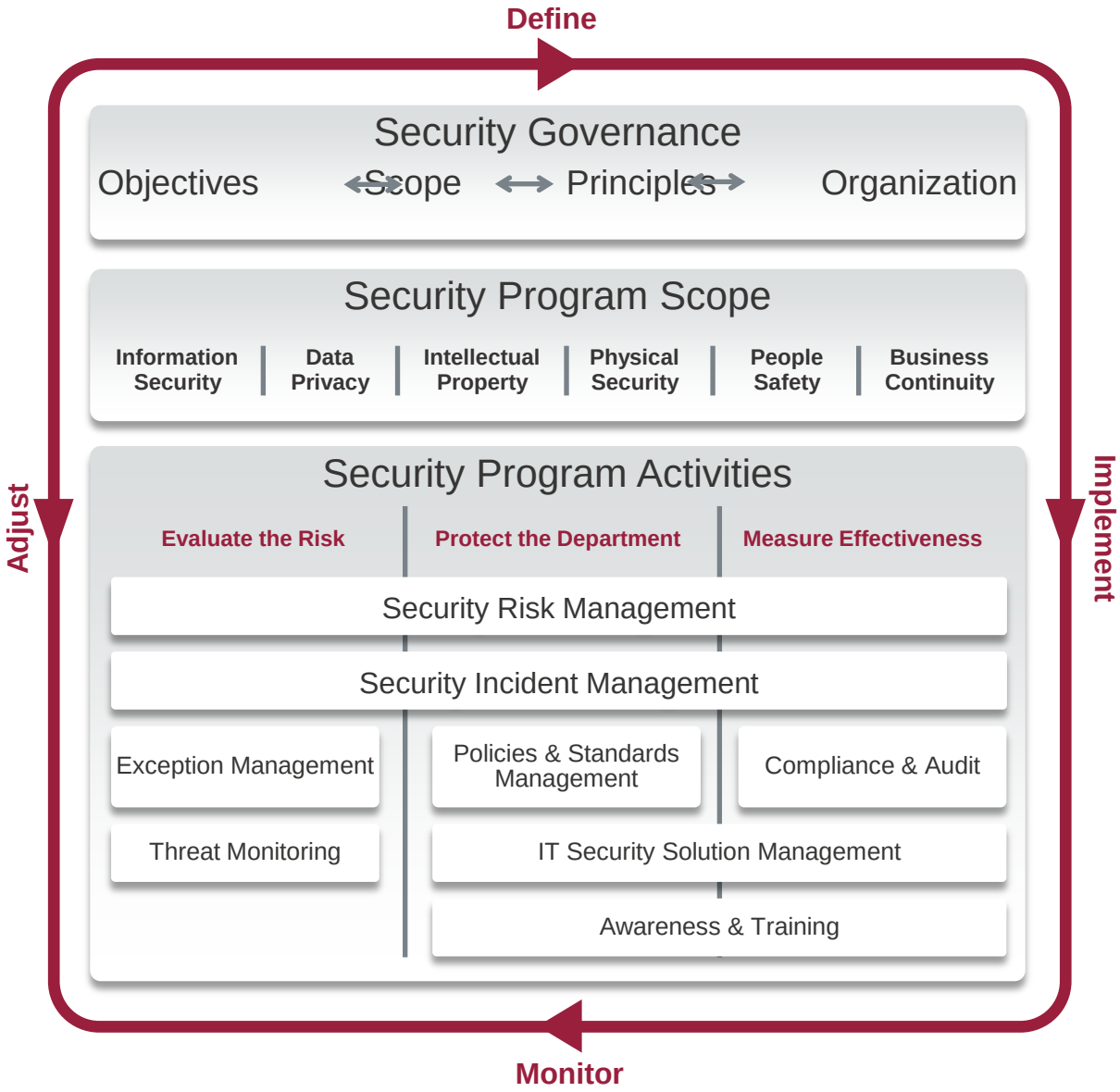




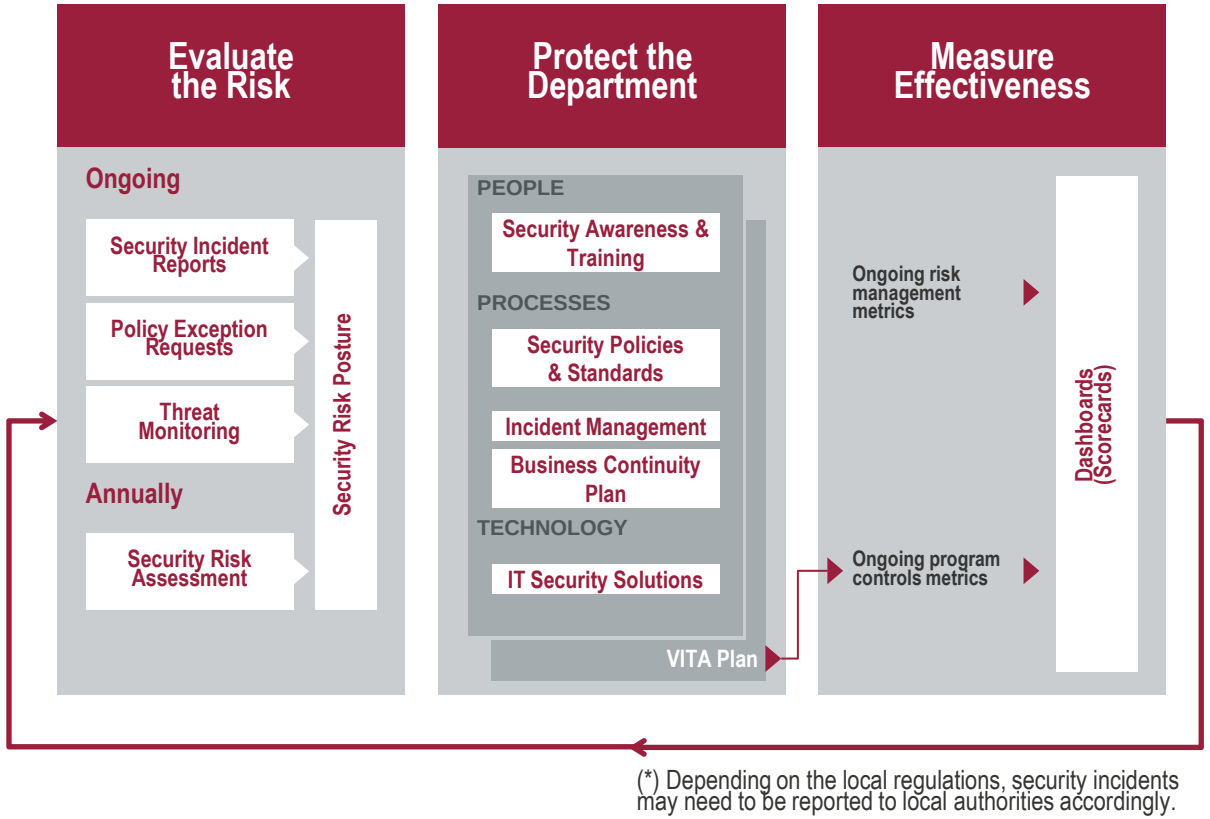
Experience the commitment®

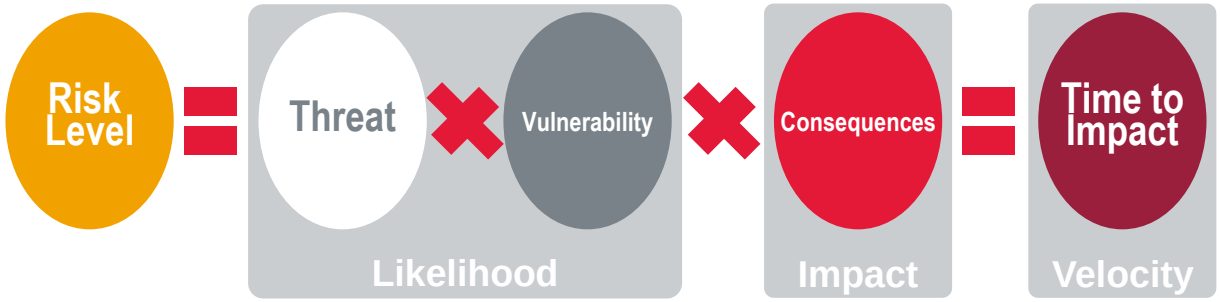
Discussion of Government Specific Security Approach and Best Practices

Agency Security Governance Framework



Agency Risk-Based Managed Security Framework





Our commitment to you

We approach every engagement with one objective in mind: to help clients succeed

Upcoming Events

Virginia Information Technologies Agency

2019 COV Security Conference

2019 Security Conference Registration and Call for Papers

Registration for the 2019 Commonwealth of Virginia (COV) Information Security Conference is now open. The 2019 conference will be held April 11-12 at the Altria Theater in Richmond. The call for papers has been issued and the conference committee is now accepting submissions.

Conference and registration information can be found on the link below.
https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/

Send your call for papers questions to: isconferencecfp@vita.virginia.gov

For all other conference questions: covsecurityconference@vita.virginia.gov

ISO/AITR Approver List

- CSRM is trying to make sure the ISO/AITR approver list for the agencies are accurate.

- If you have questions or want to verify the approvers listed for your agency contact:

Tina.Harris-Cunningham@vita.virginia.gov

IS Orientation

The next IS Orientation will be held in March. More information will be forthcoming.

Future ISOAG

Feb. 6 , 2019 @ CESC 1-4 p.m.

Speakers: Roy Logan, NASA

Carlos Rivero, Office of Secretary of Administration

TBA, Google Cloud

ISOAG meets the first Wednesday of each month in 2019

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk