



# Into the cybersecurity breach

**Tim Sanouvong**  
State Sector Cyber Risk Services  
Deloitte & Touche LLP

April 3, 2015



# Agenda

- Setting the stage — Cyber risks in state governments
- Cyber attack vectors
- Preparing for a breach: **Becoming Secure.Vigilant.Resilient.™**
- Lessons learned post-breach

# Cyber risks in state governments

# The cyber threat landscape

- Cyber attacks have evolved into very **sophisticated attacks** fueled by **profit motive**, **geopolitics**, and **political activism**
- Connectivity is significantly increasing via the **Internet of Things**, providing new attack channels
- Governmental and industry **regulations and standards** are increasingly addressing the growing cyber threat and risks to our Nation's economy and national security
- Significant **rise in Supervisory Control and Data Acquisition (SCADA) hacking** across various industries and systems



**92%**  
of breaches are perpetrated by outsiders



**14%**  
of breaches are by insiders and are rising



# State governments are a target...

## Citizen trust impact is a top concern



**States collect, share and use large volumes of the most comprehensive citizen information.**

Cyber incidents impact state business by affecting citizen services, revenue collections, or result in unplanned spending. In addition, the impact to citizen trust could have a significant consequence.

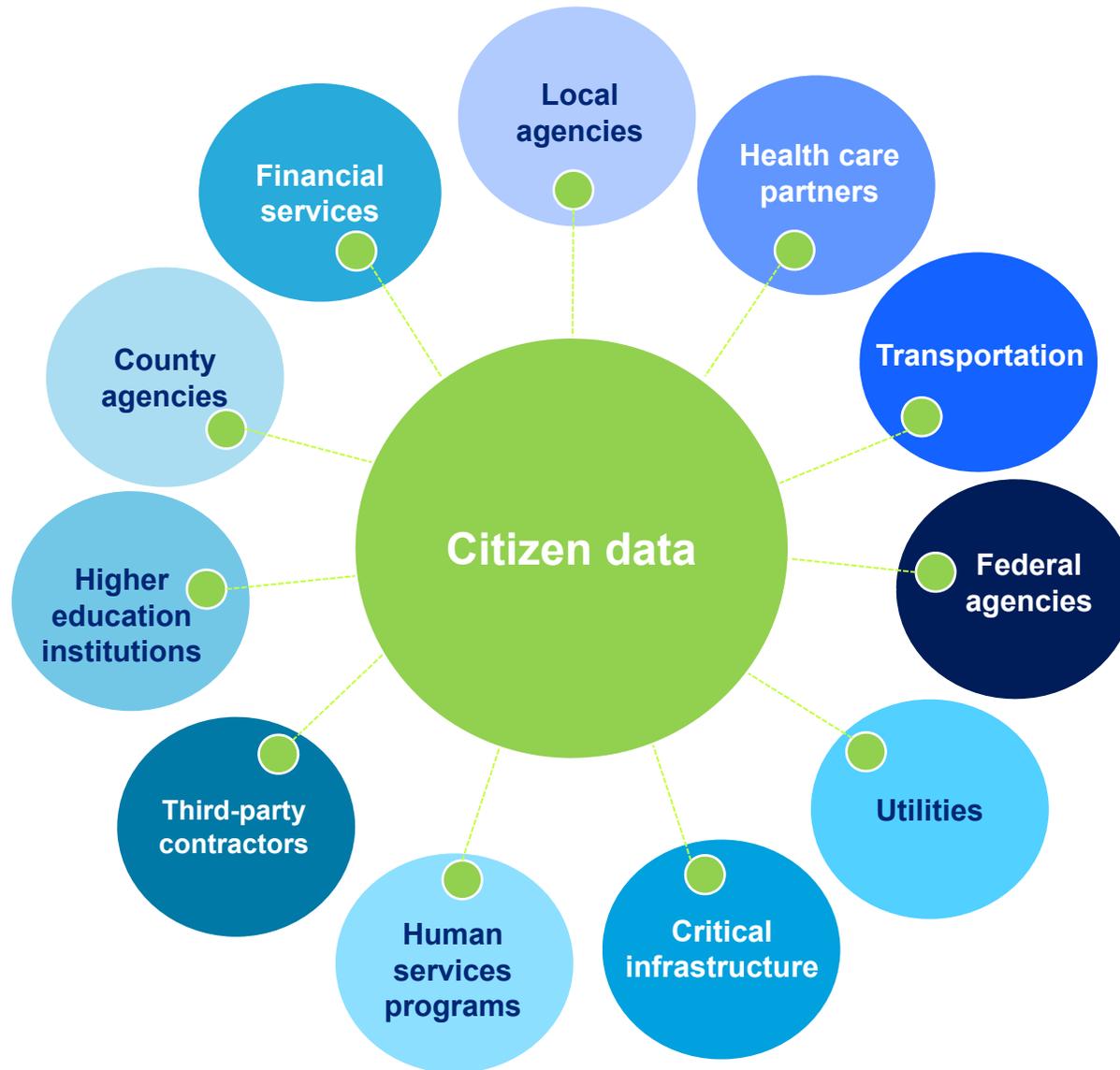


**This volume of information makes states an attractive target for both organized cyber criminals and hactivists.**



**Cybersecurity responses are most effective when coordinated at the Governor or business executive level**

# Citizen data is a component in every facet of business



# Cyber attack vectors

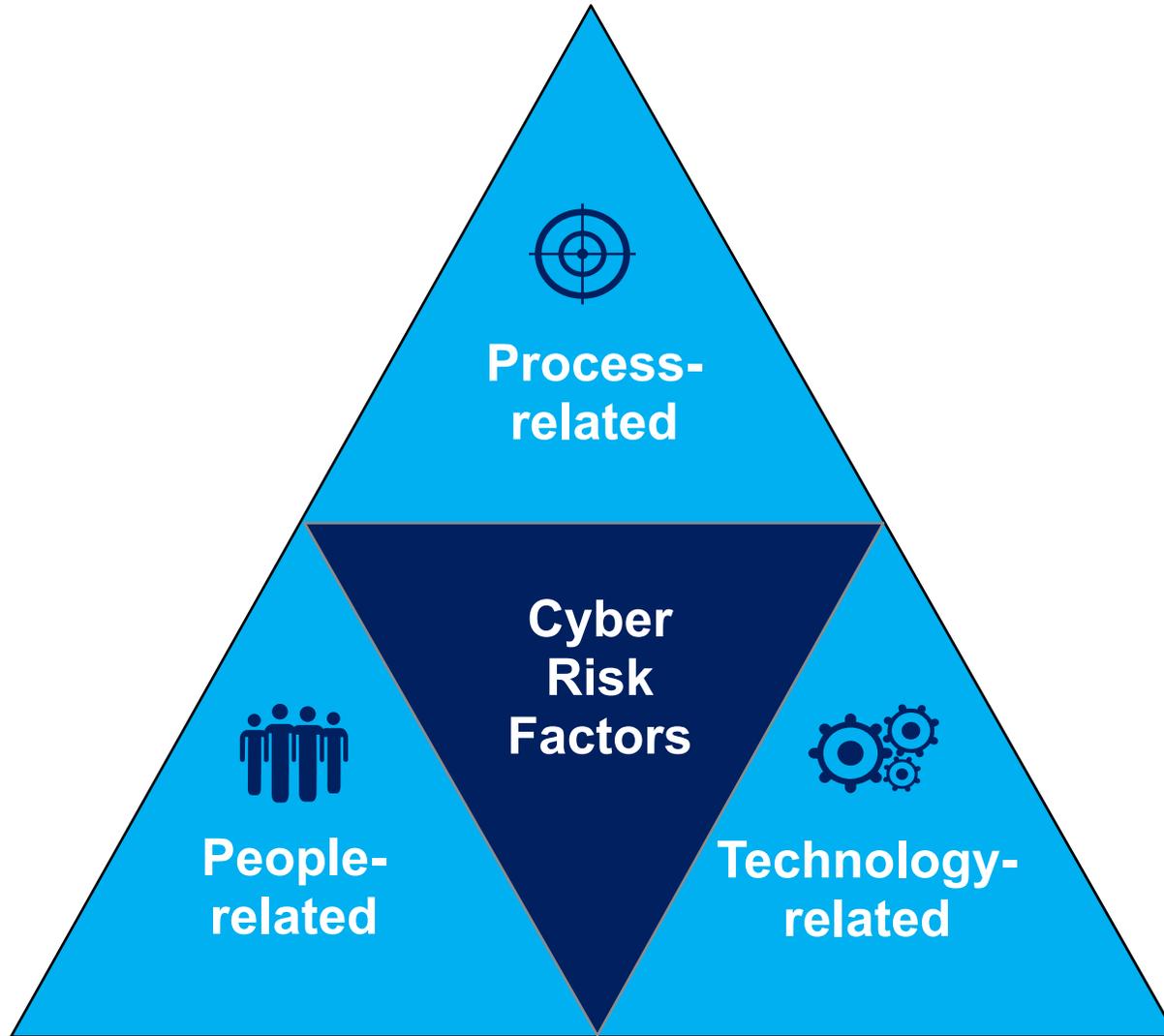
# Five common attack vectors

Organizations need to identify emerging risks as part of an effective, integrated governance, risk and assurance program.

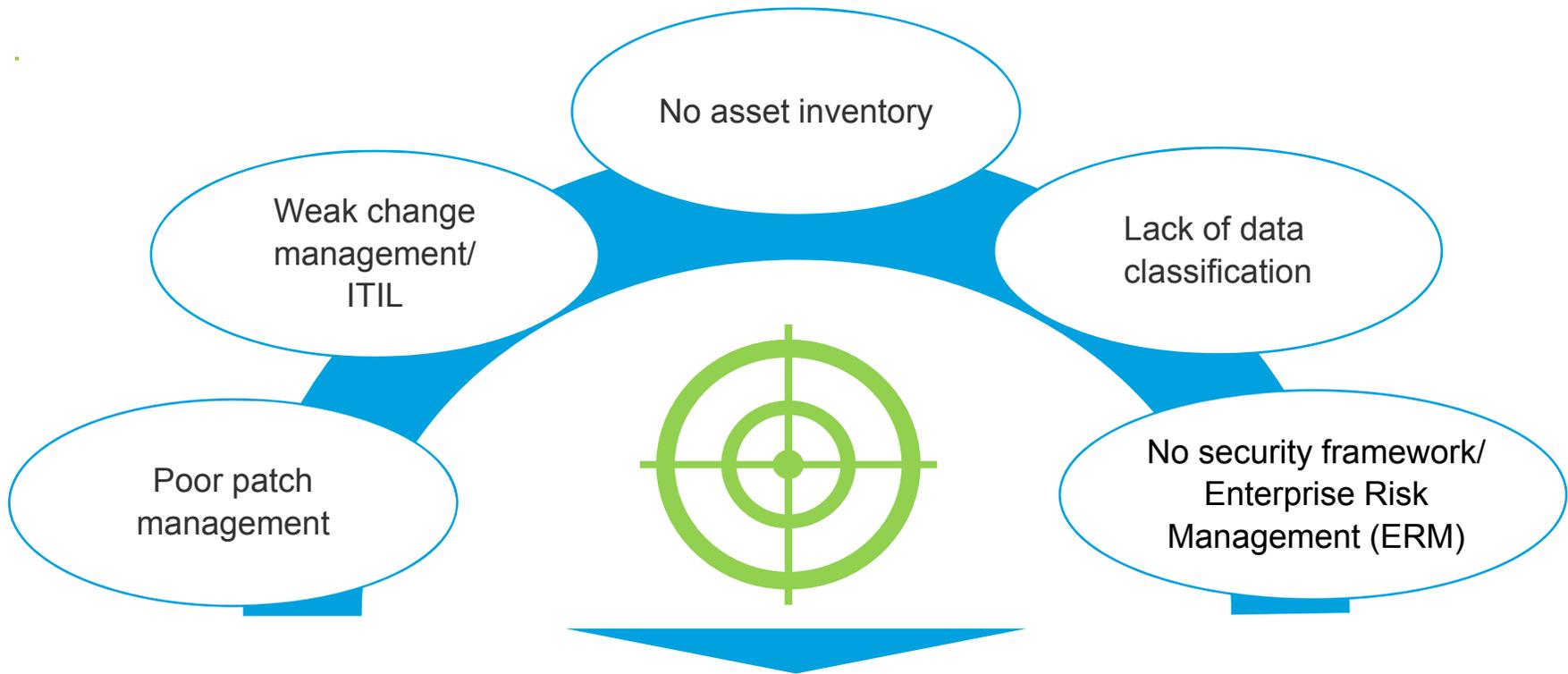


***These vectors are not only important individually; when combined, they are critical***

# Factors in managing cyber risks

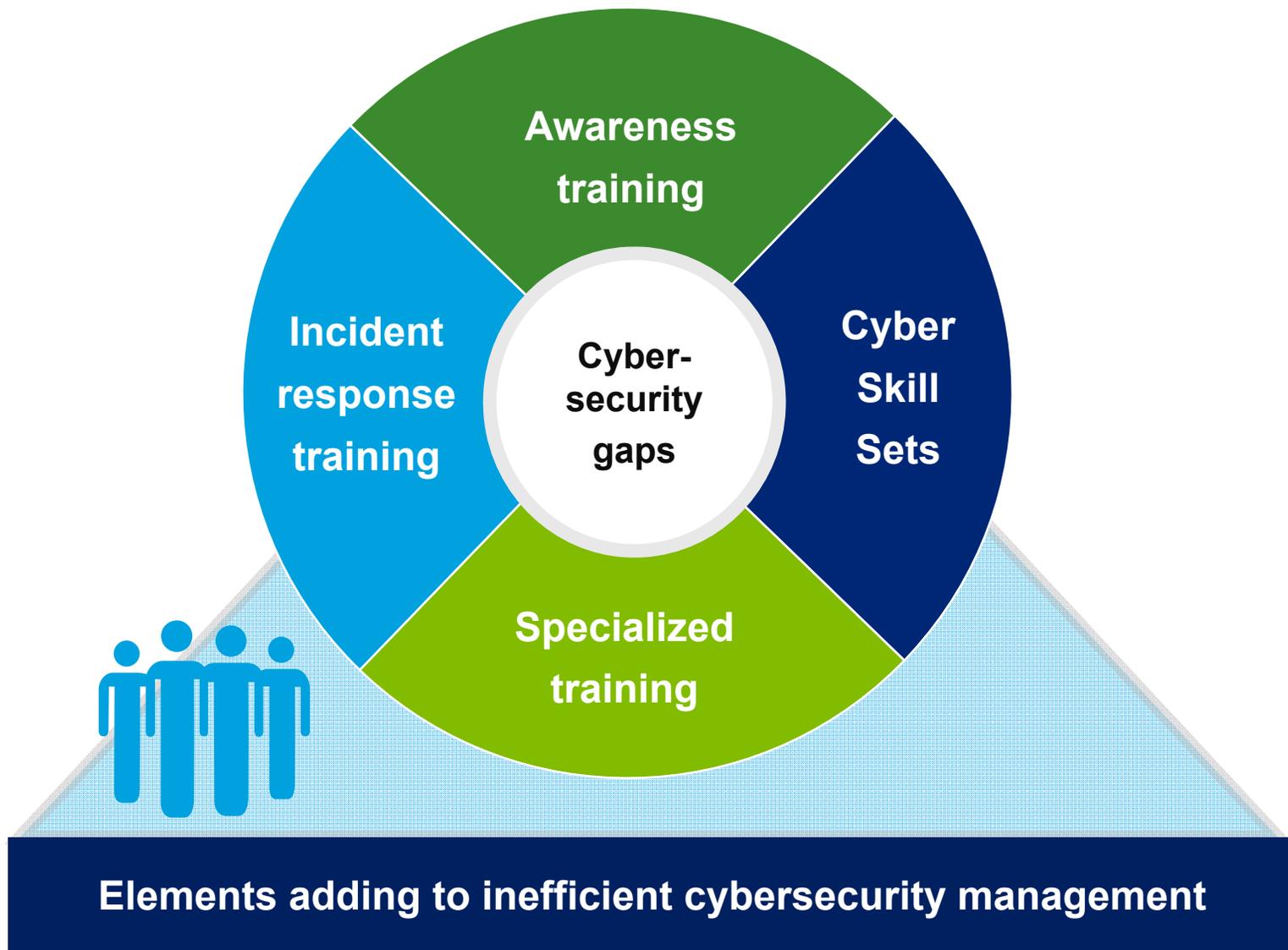


# Process-related factors

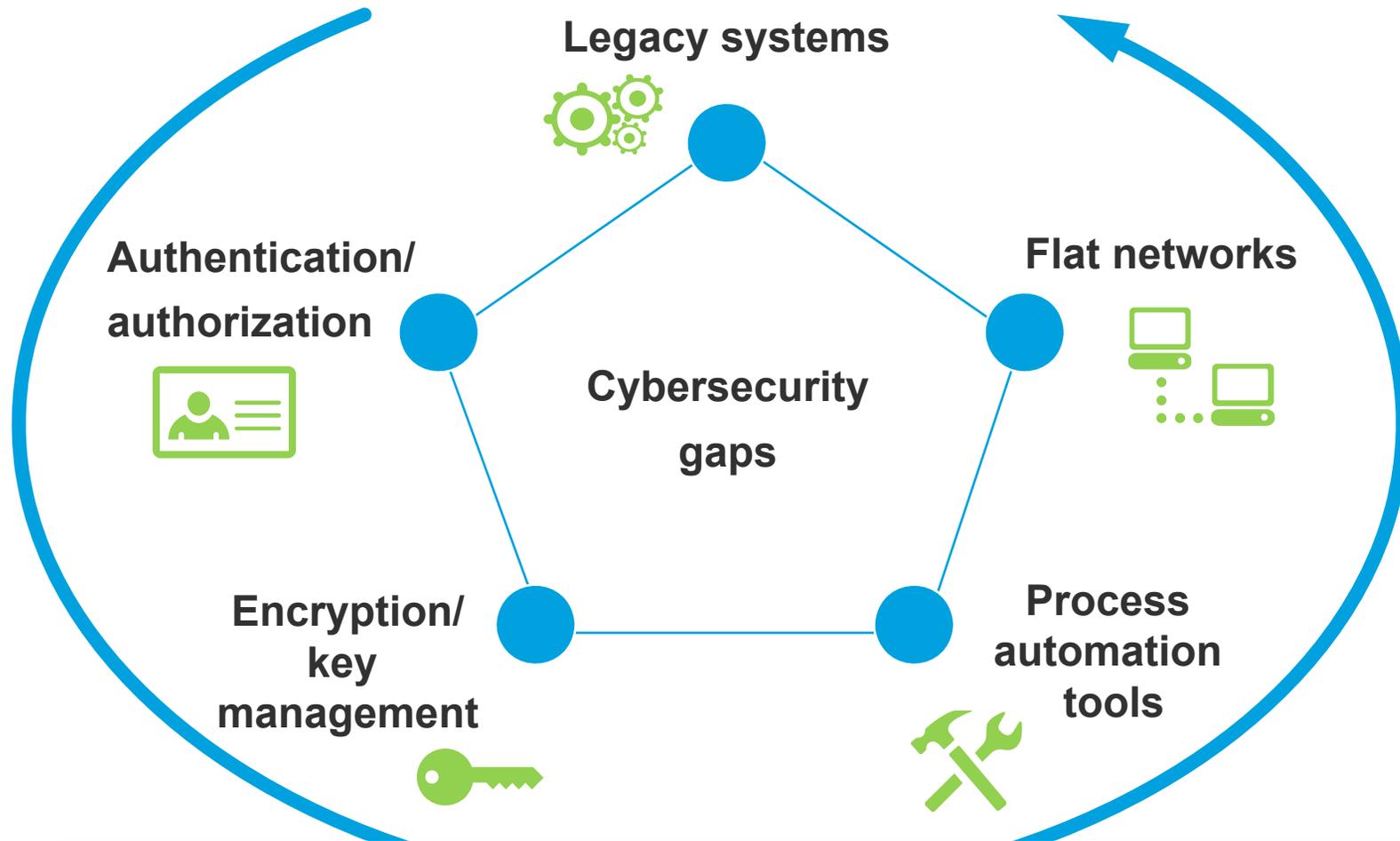


**Elements adding to inefficient cybersecurity management**

# People-related factors



# Technology-related factors



**Elements adding to inefficient cybersecurity management**

# Common symptoms of hacker penetration

Unexplained occurrences could signify a potential breach:

- Network traffic characteristics:
  - Large volumes of encrypted data outbound from the network
  - Connections to a-typical geographic locations
  - Denial of service attack
- System characteristics:
  - Decreased system performance and capacity
  - Increase in authentication and authorization exceptions
  - Increases in system error conditions
  - Increases in relatively static file sizes
- Discrepancies involving customer and/or company accounts
- Call from the FBI or US Secret Service

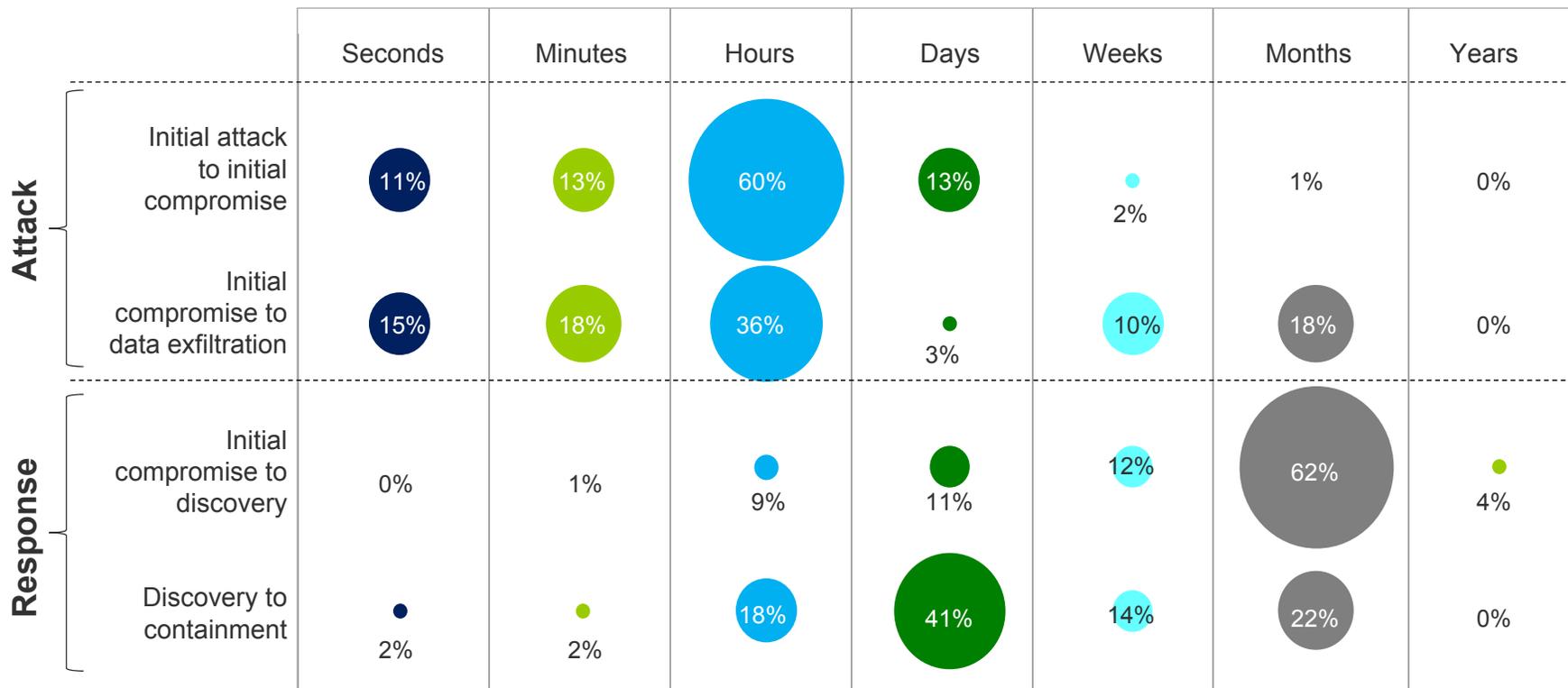
# Preparing for a breach:

Becoming

Secure.Vigilant.Resilient.™

# Speed in detection is critical

While it is not possible to prevent all cyber attacks, you can significantly limit damage by quickly detecting and dealing with a compromise.



Source: Verizon 2013 Data Breach investigations Report

Copyright © 2015 Deloitte Development LLC. All rights reserved.

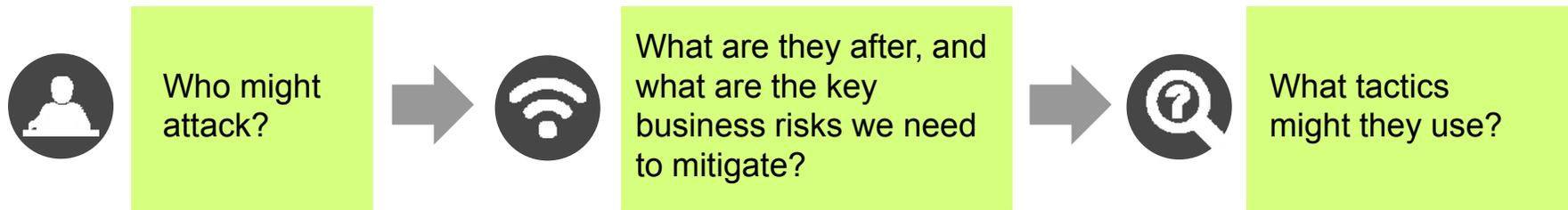
# Ask the right questions

Better understand cyber risks to the business and citizen trust to your state environment:

- Where are my high-risk assets?
- Where does the data reside?
- What are the citizen privacy issues?
- Why does the citizen data need to be protected?
- What are the possible motives of an attack based?
- What is the business implication of a breach within the agency, state and external parties?
- What systems are in place to manage risks and where are they?



# Understand threats and motives relevant to your environment



IMPACTS \ ACTORS	IMPACTS							
	Financial theft/fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infra-structure	Reputation damage	Threats to life safety	Regulatory	
Organized criminals	Very high	Low	Low	Low	High	Low	Moderate	
Hactivists	Low	Low	Very high	Low	Very high	Low	Moderate	
Nation states	Low	Low	Very high	Very high	Low	Very high	Moderate	
Insiders/partners	Very high	Low	High	Low	High	Low	Moderate	
Skilled individual hackers	Moderate	Low	High	Low	High	Low	Moderate	

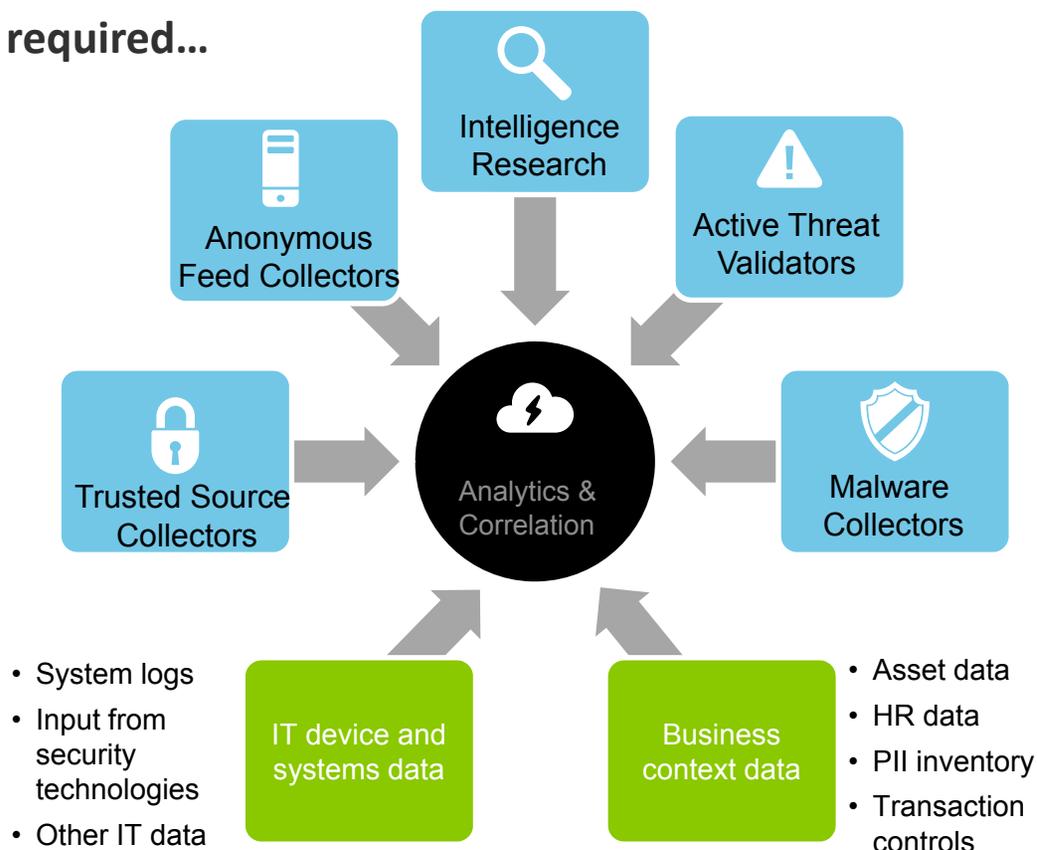
**KEY**   ■ Very high   ■ High   ■ Moderate   ■ Low

# Incorporate threat intelligence

Threat data, alone, does not enable detection

**A range of threat “indicator” data is required...**

- Phishing URL/email blacklists
- Trojan/botnet watch lists
- Suspicious domain registrations
- Infected IPs from malware victims
- Honeypot threat intelligence
- C&C/botnet communications monitoring
- Phishing dropsite monitoring
- Malicious nameserver watch lists
- DNS monitoring
- Cloud-based validation scanners
- Fast flux monitoring
- Dynamic DNS communication
- HTTP Referrer and User Agent Profiling
- Social media monitoring



... but detecting today's threats and supporting efficient incident response and analysis requires correlation with data from the IT environment...

... and other forms of business and reference data.

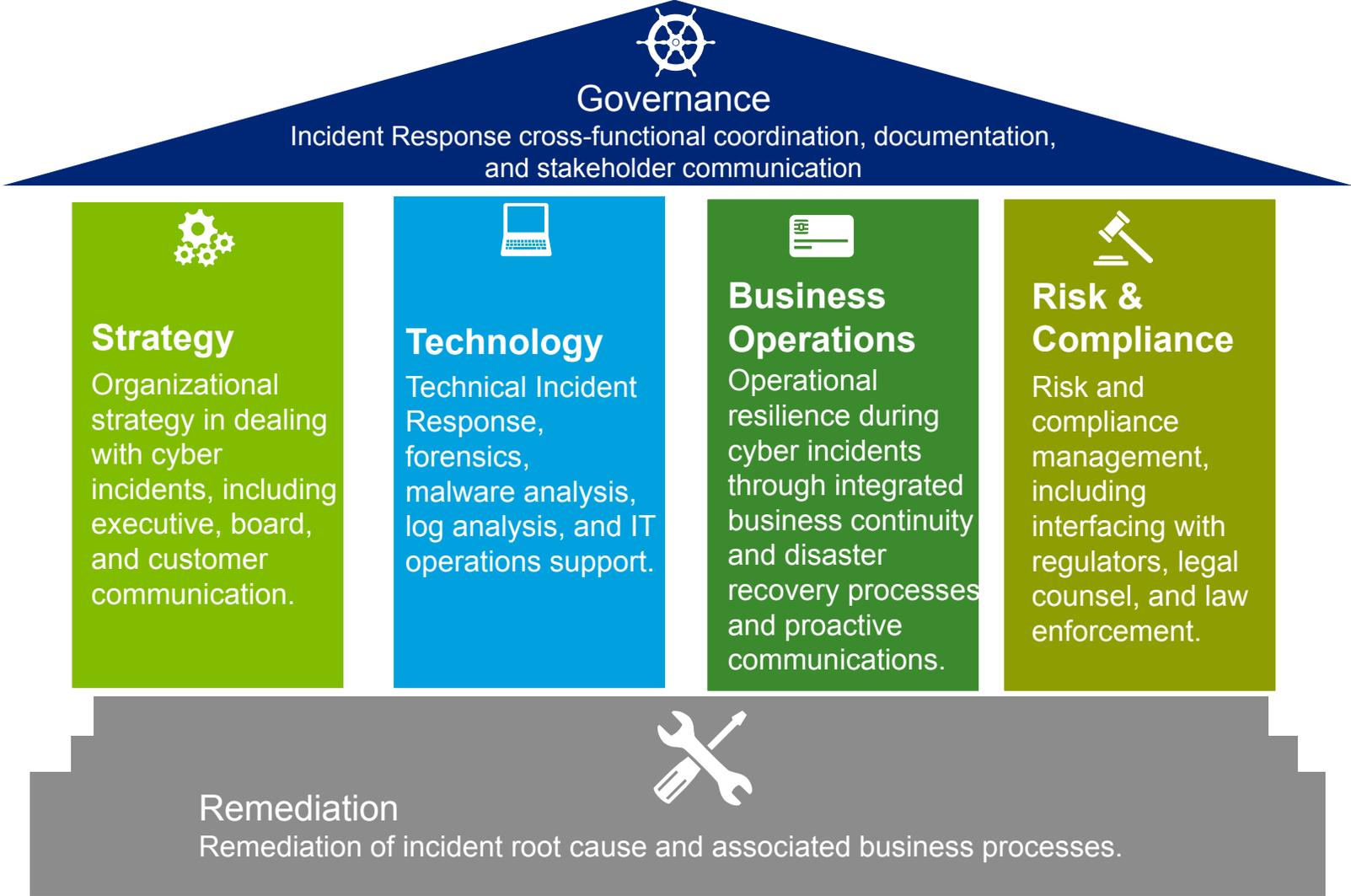
# Build a resiliency program as an opportunity to engage with the business



# Lessons learned post- breach

# Incident response programs require coordination

Organizations should embrace a broad Incident Response approach across disciplines, stakeholders and environments



# Secure.Vigilant.Resilient.™ security program establishment

## SECURE

Establish risk-prioritized controls to protect against known and emerging threats, and comply with standards and regulations

### ***Cyber threat risk assessment***

Identify threats and potential vulnerabilities to assess risks to critical infrastructure and assets. Develop risk remediation measures to mitigate risks to acceptable levels and execute through a strategic initiative roadmap.

## VIGILANT

Establish situational risk and threat awareness across the environment to detect violations and anomalies

### ***Cyber event monitoring***

Design and implement cyber threat monitoring capabilities and security event management systems to correlate information and detect potential incidents.

## RESILIENT

Establish the ability handle critical incidents, quickly return to normal operations, and repair damage to the business

### ***Cyber threat war gaming***

Establish "muscle memory" and multi-function coordination to better manage the business crises that cyber incidents can cause.

### ***Cyber threat response***

Establish crisis and incident management plans to escalate, communicate and respond to incidents in a coordinated, efficient and timely fashion. Regularly test the ongoing effectiveness of plans through simulation for improvement opportunities.

Question & answer

# Contact info

Tim Sanouvong  
State Sector Cyber Risk Services  
Deloitte & Touche LLP  
[tsanouvong@deloitte.com](mailto:tsanouvong@deloitte.com)

 Connect with me on LinkedIn

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

# Deloitte.



Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.

As used in this document, "Deloitte" means Deloitte & Touche LLP-Consulting LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2015 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu Limited