



ISOAG Meeting November 4, 2015

Welcome to CESC!





ISOAG November 4 , 2015 Agenda

- | | |
|----------------------------------------------------------------|----------------------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Understanding cyber threat landscape & data classification | Tim Sanouvong & Swapan Arora, Deloitte |
| III. Upcoming Events | Bob Baskette/Mike Watson, VITA |
| IV. Partnership Update | Bob Baskette, VITA / Michael Clark, NG |



Understanding cyber threat landscape & data classification

Tim Sanouvong & Swapan Arora

Public Sector – Cyber Risk Services
Deloitte & Touche LLP

November 4, 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
- Understanding data classification
- Data classification framework & process

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



Source: 2013 Verizon Data Breach Investigations Report with the U.S. Secret Service, FBI, Deloitte, DHS and others
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

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

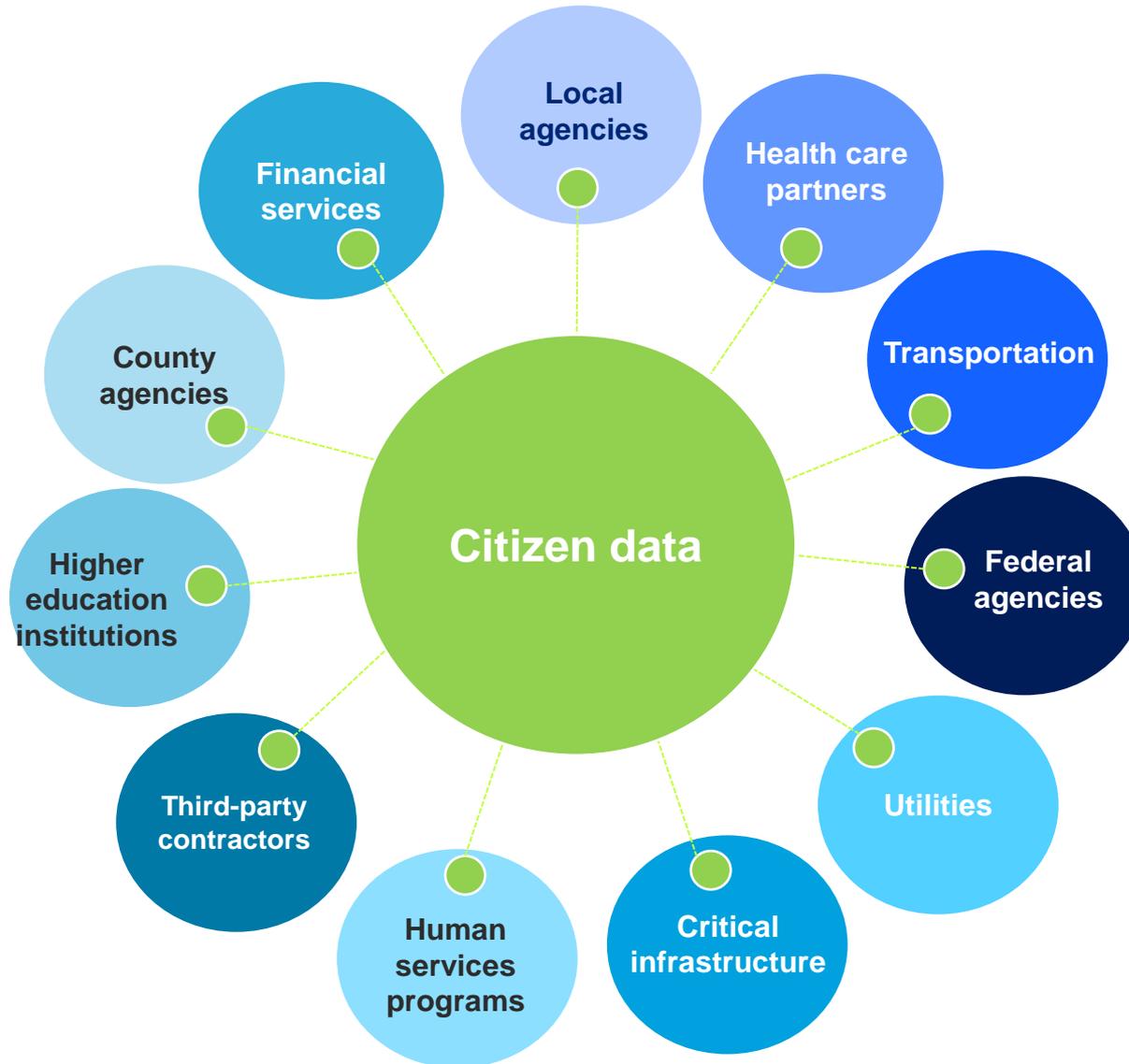


This volume of information makes states an attractive target for both organized cyber criminals and hackers



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

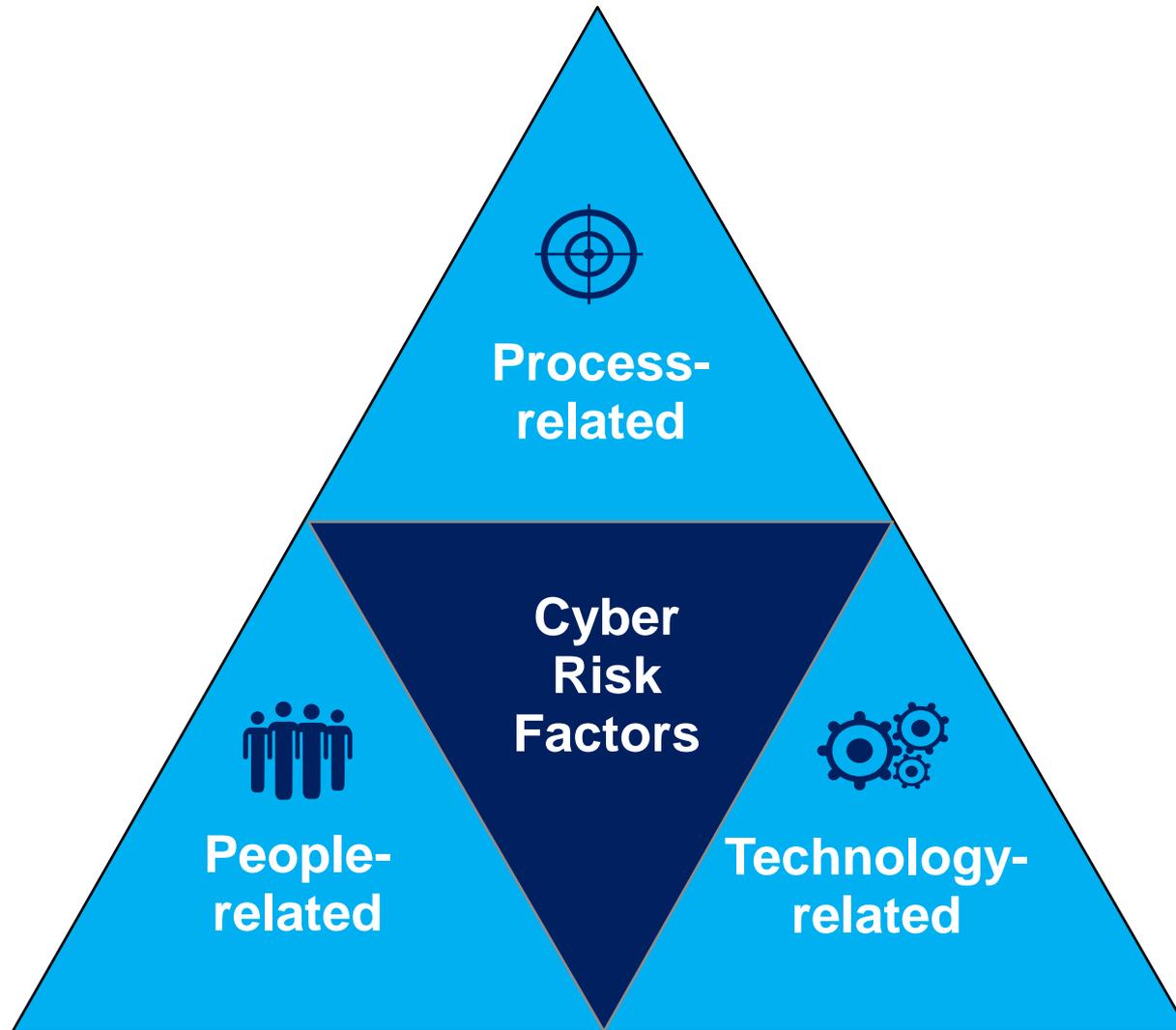
Five common attack vectors

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

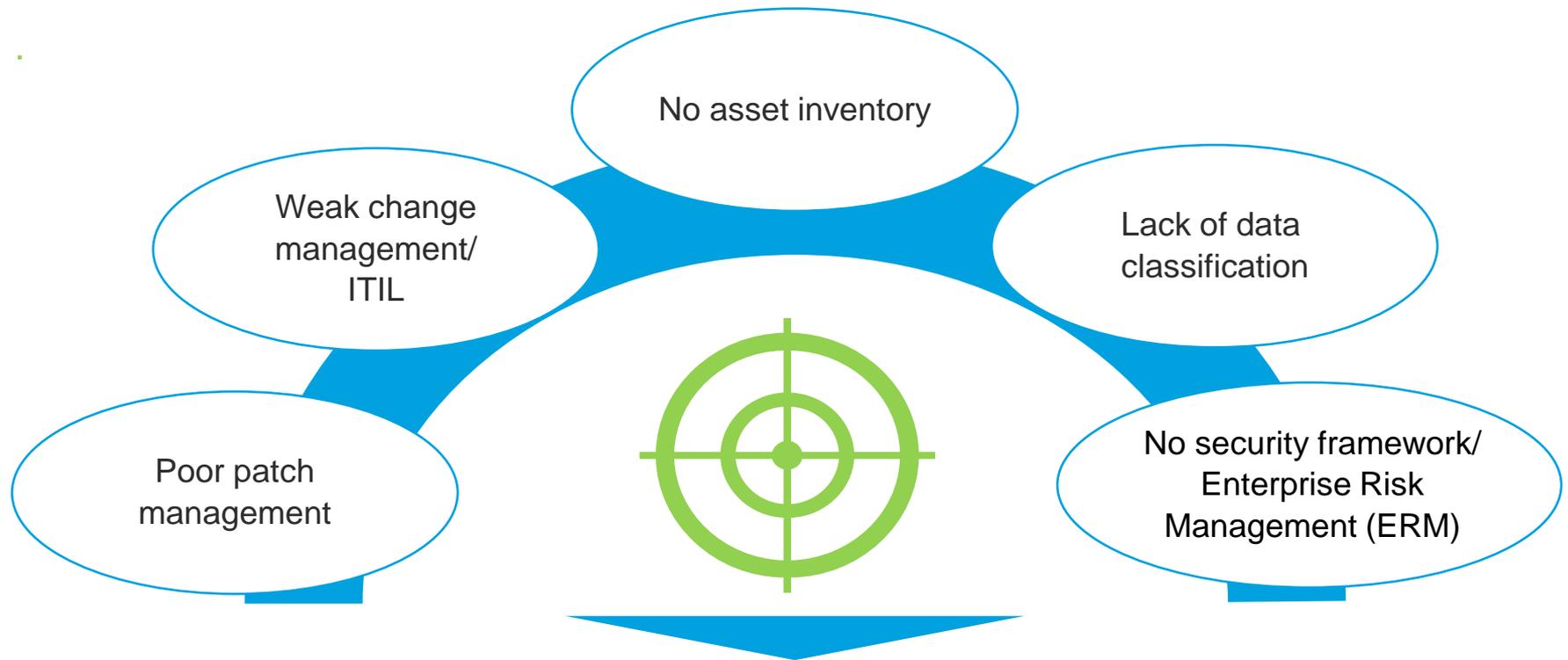


These vectors are not only important individually; when combined, they are critical

Factors in managing cyber risks

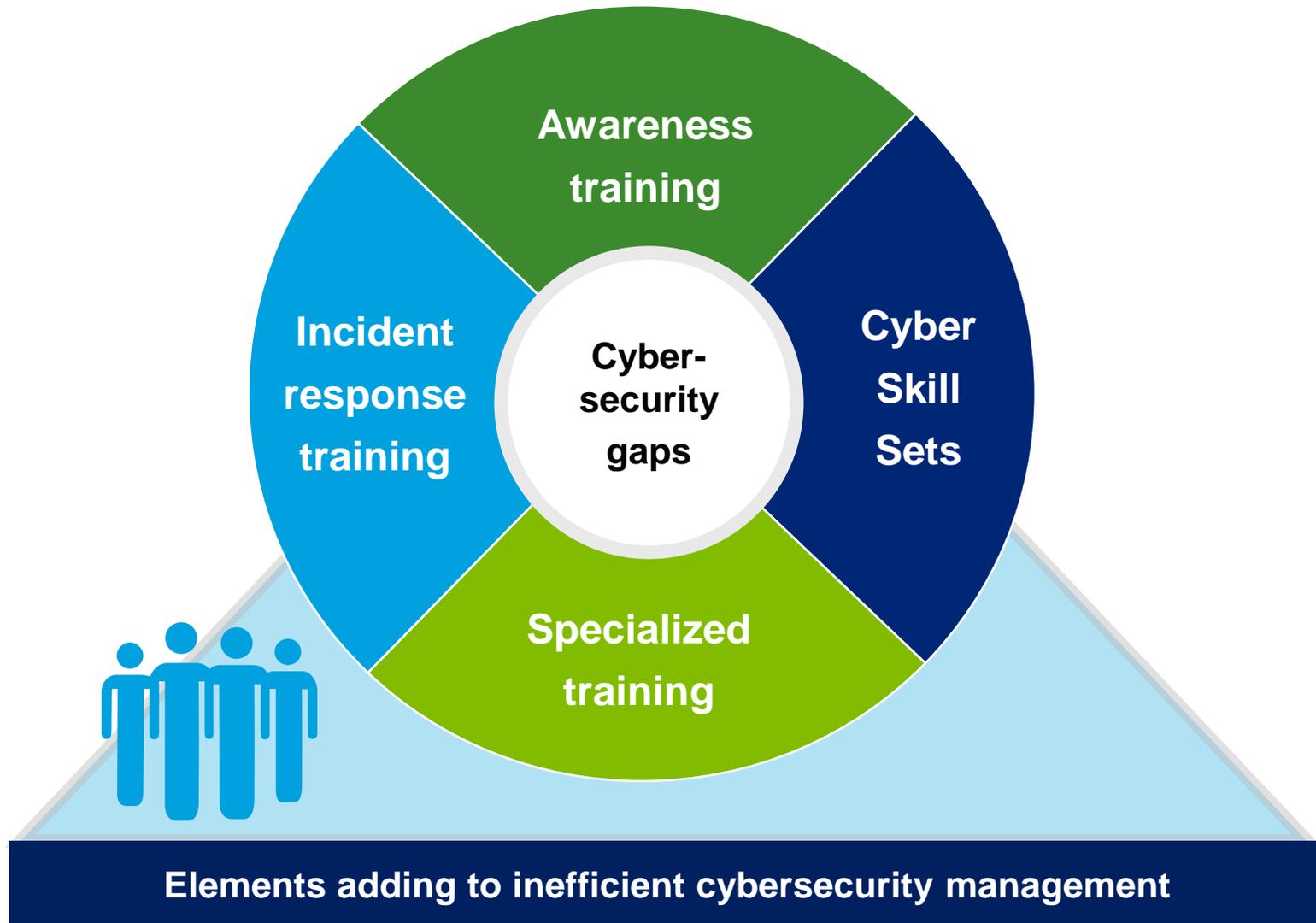


Process-related factors

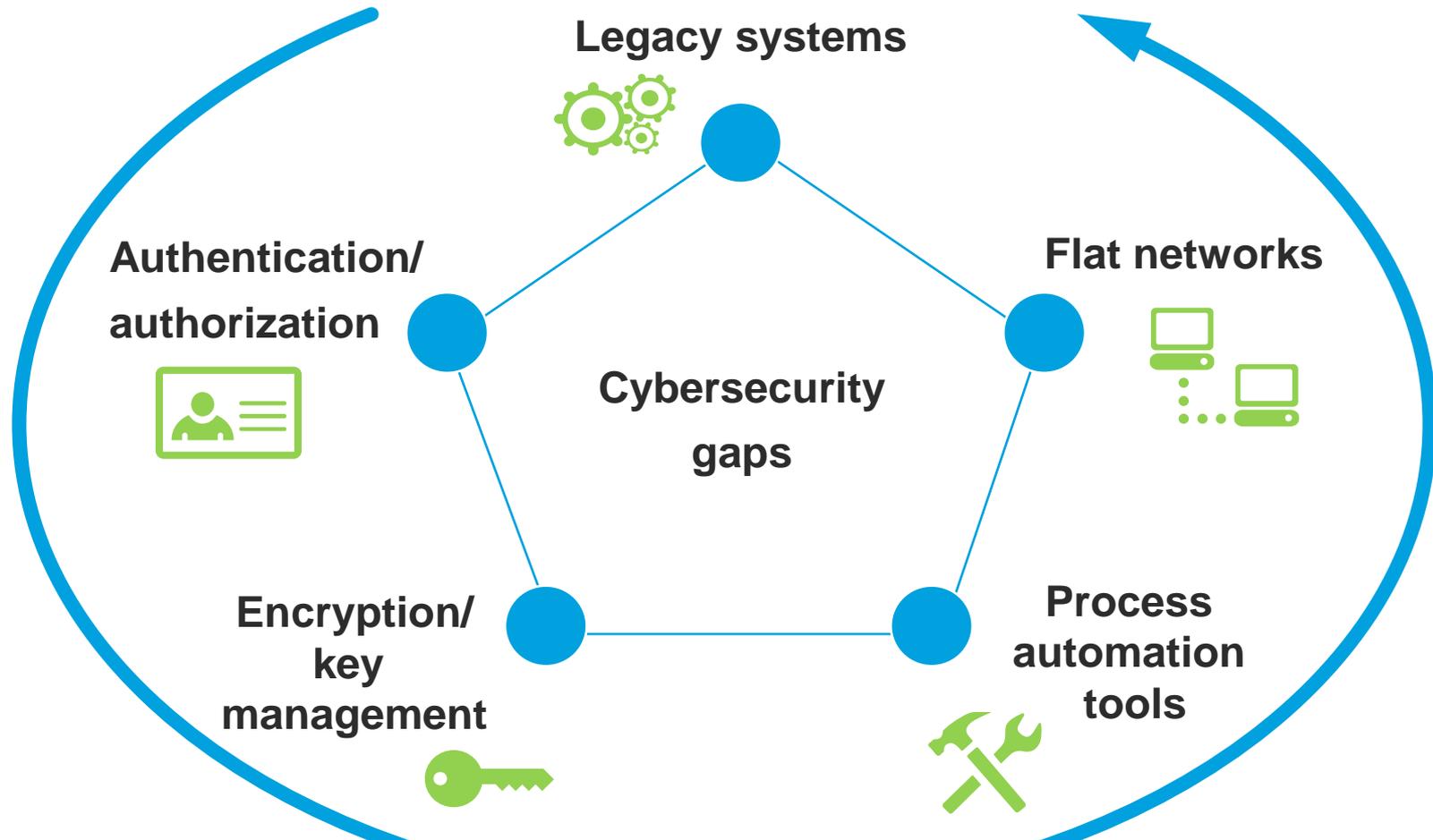


Elements adding to inefficient cybersecurity management

People-related factors



Technology-related factors



Elements adding to inefficient cybersecurity management

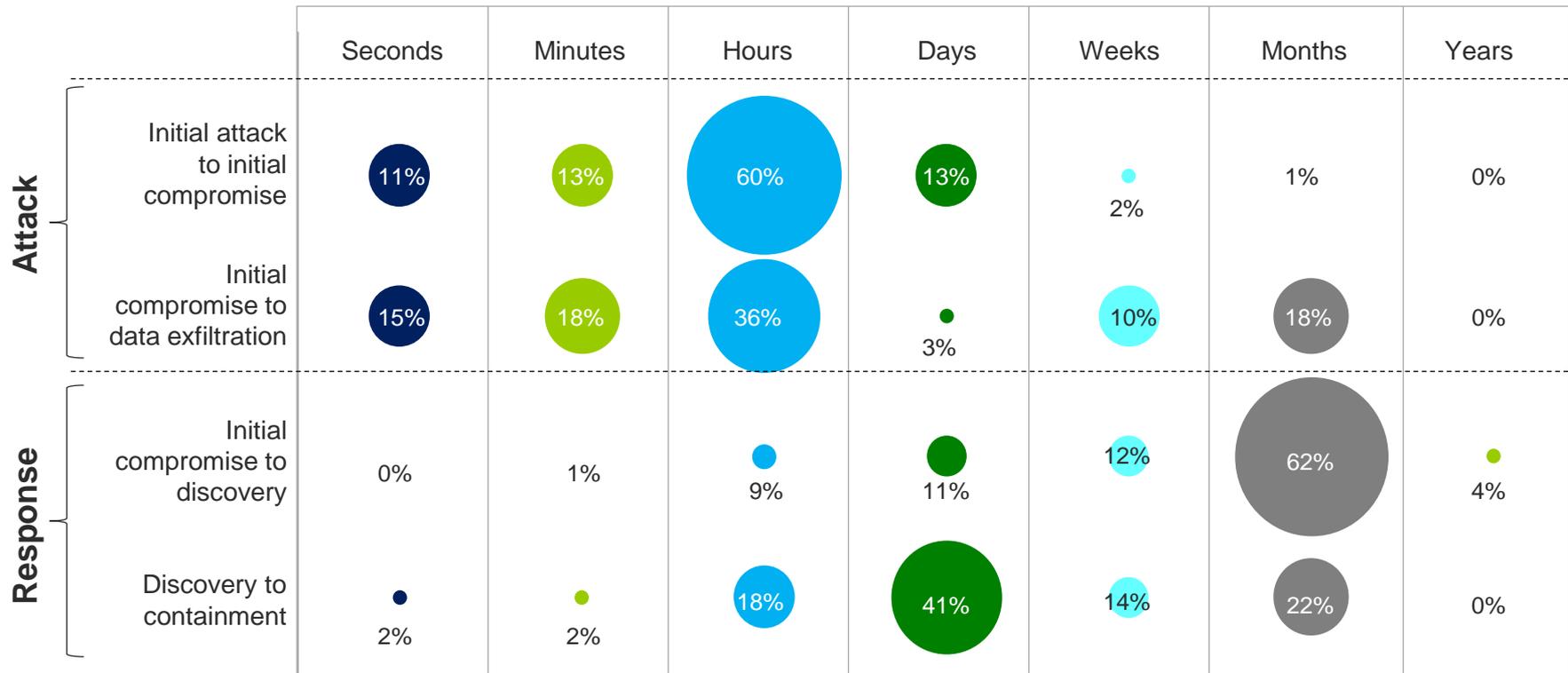
Preparing for a breach:

Becoming

Secure.Vigilant.Resilient.TM

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...

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

- What are my high-risk assets?
- 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?

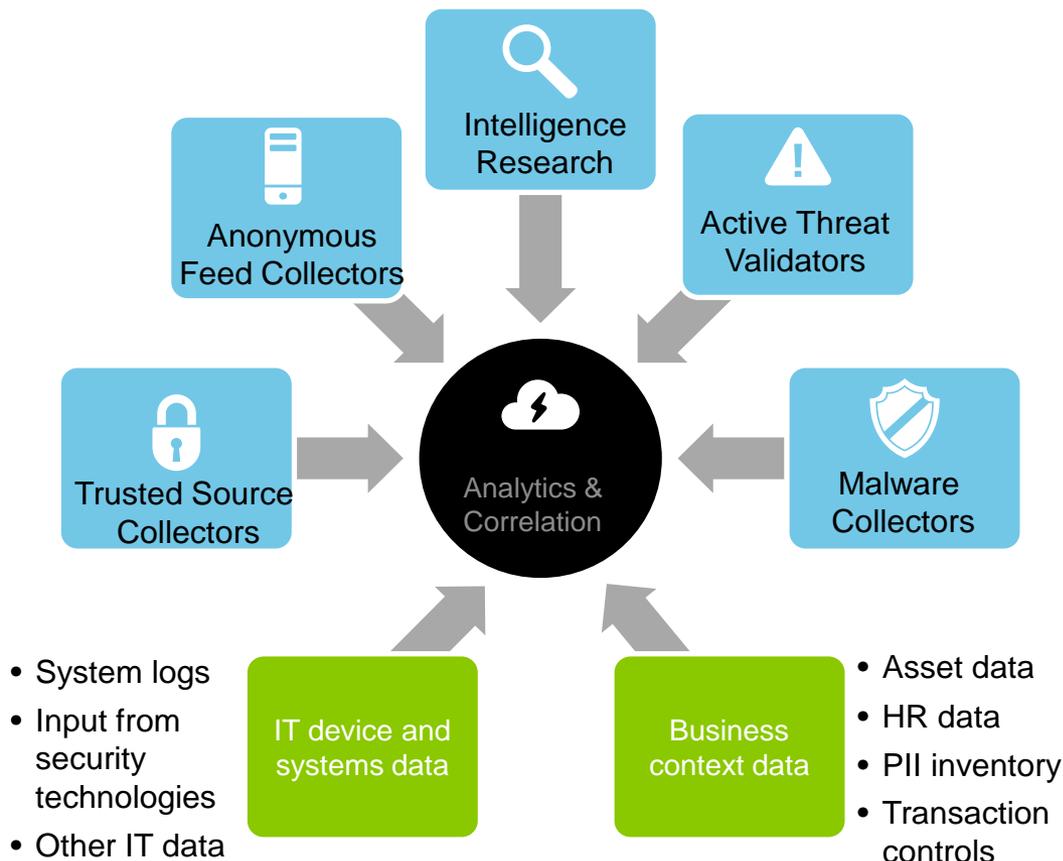


Incorporate threat intelligence

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

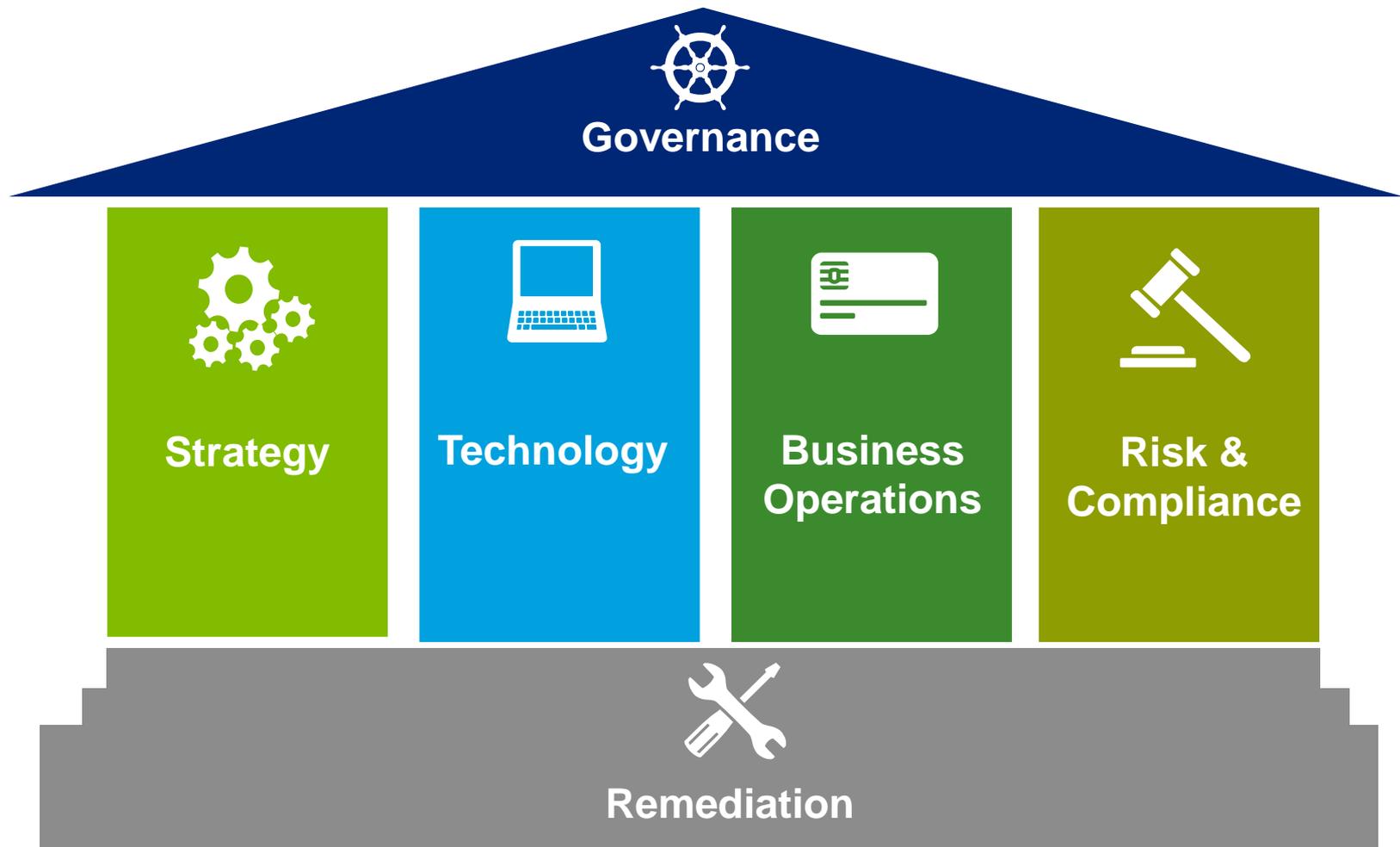


... and other forms of business and reference data.

Lessons learned post- breach

Incident response programs require coordination

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



What's your next move?

Take a programmatic approach, communicate and practice

Secure

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

Cyber threat risk assessment

Vigilant

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

Cyber event monitoring

Cyber threat response

Resilient

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

Cyber threat war gaming

Data classification strategy

Understanding data classification

Information security is nearly impossible without correct information classification.

Objectives

- Define the requirements for classifying and securing an organization's information
- Determine what information can be disclosed to non-employees, as well as that should not be disclosed outside of the organization
- Design information security controls around information that is processed, transmitted, and stored

Problem

- Confidential and sensitive information may be handled in an inappropriate and insecure manner
- Customer or employee related information, or financial information may be disclosed to unauthorized individuals
- Privacy and other regulatory laws might be breached, which may lead to financial losses or negative publicity

Different data classifications

Data classification and allocation of responsibilities can help ensure that the most valuable information assets have the highest level of protection.

1 Public Information



- No authentication or authorization requirements and is freely available to the general public with ease through the use of the Internet and other media sources.

2 Business Use Information



- Intended for use by associates when conducting company business. All information should be considered Business Use Information by default, and when warranted and necessary it should be classified as Public Information, Confidential Information, or Restricted Information.

3 Confidential Information



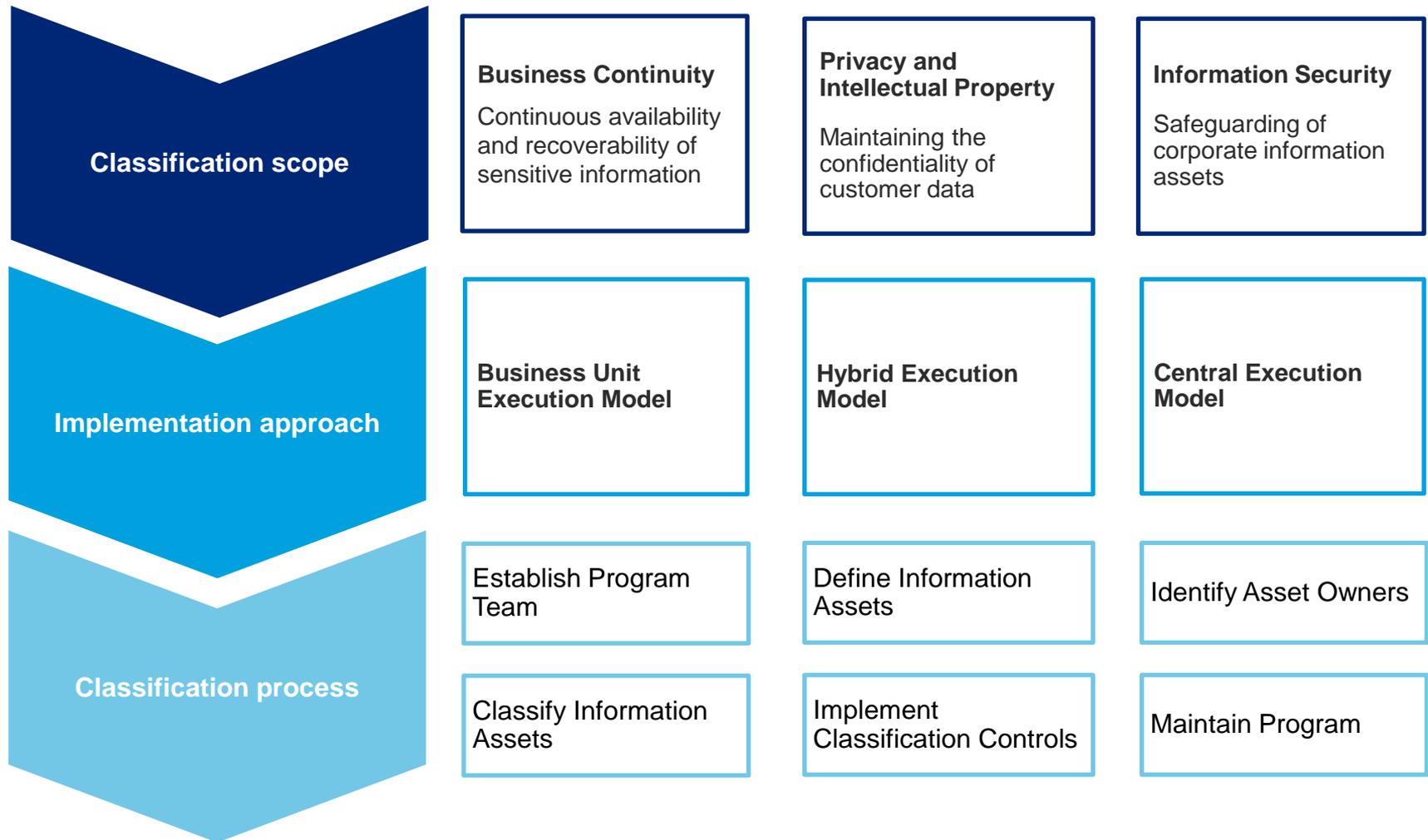
- Sensitive internal information that is restricted based upon job responsibility. Unauthorized disclosure would have an adverse impact to the organization, its customers, its associates, or its business partners.

4 Restricted information



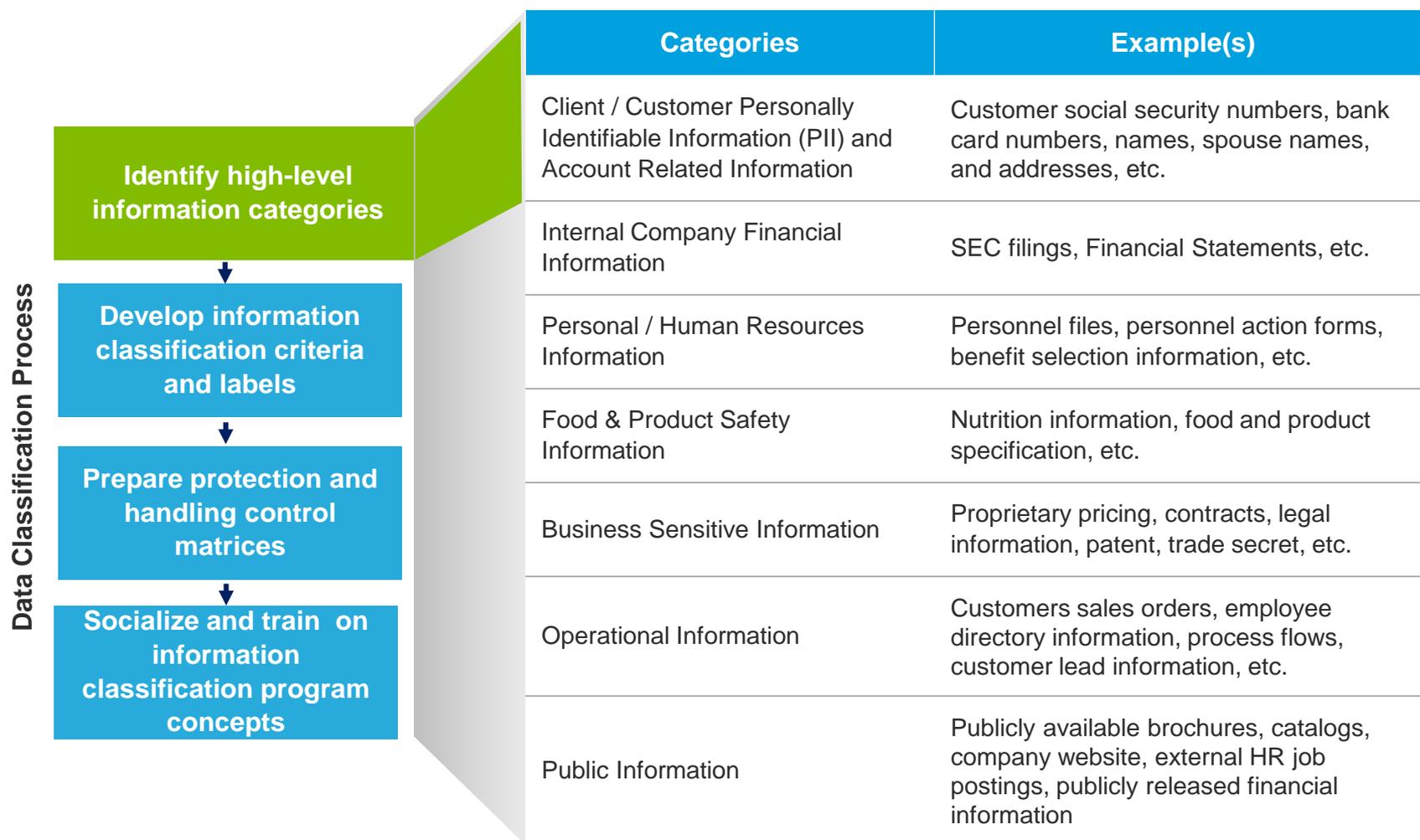
- Information that has strict limitations placed upon its internal access and external disclosure due to the critical nature of the information – Restricted Financial Information, Restricted Personal Information, and Restricted Customer Proprietary Network Information (CPNI).

Data classification framework



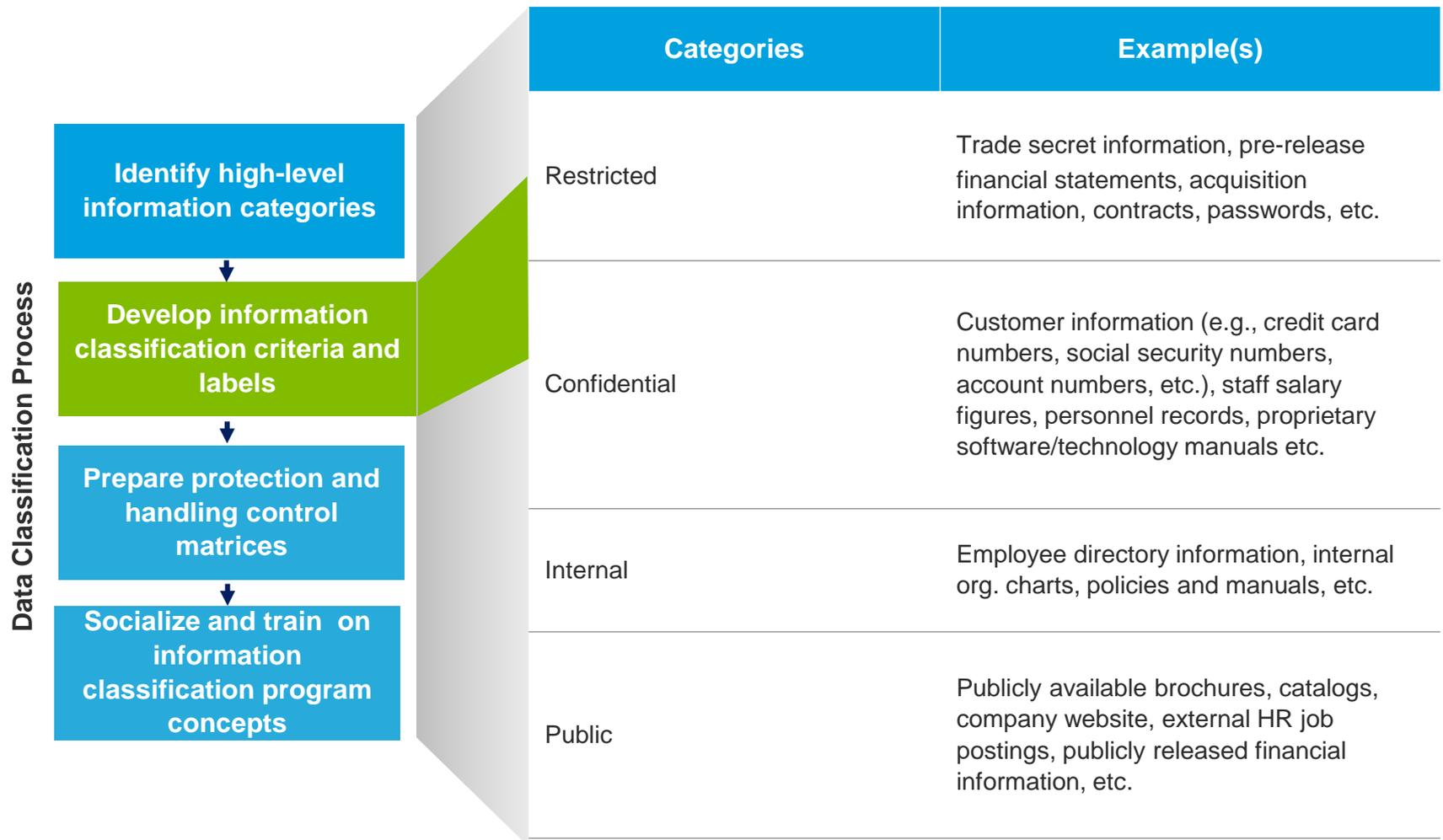
Data classification process

Step 1: Identify high-level information categories



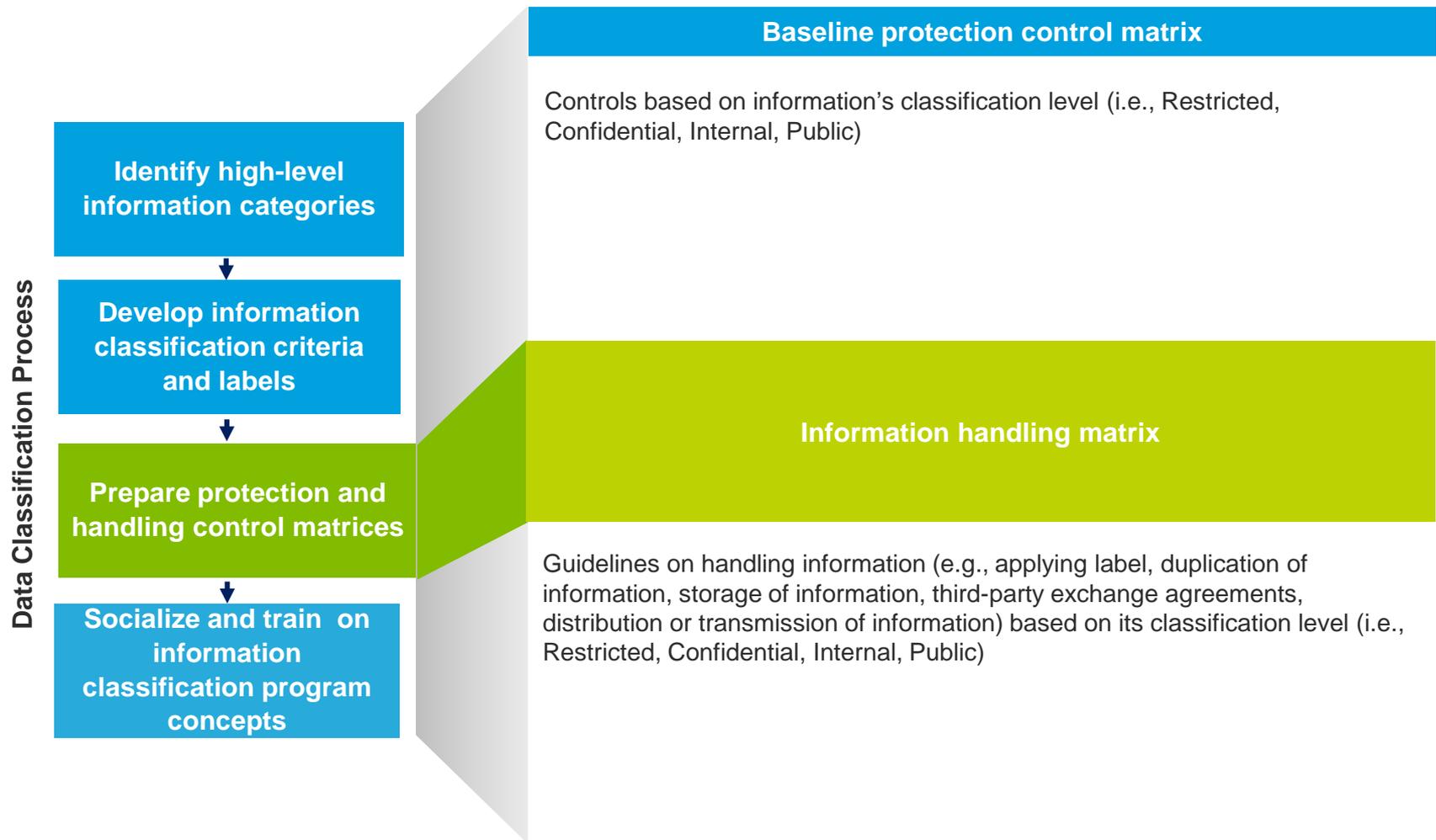
Data classification process

Step 2: Classify information and label assignment



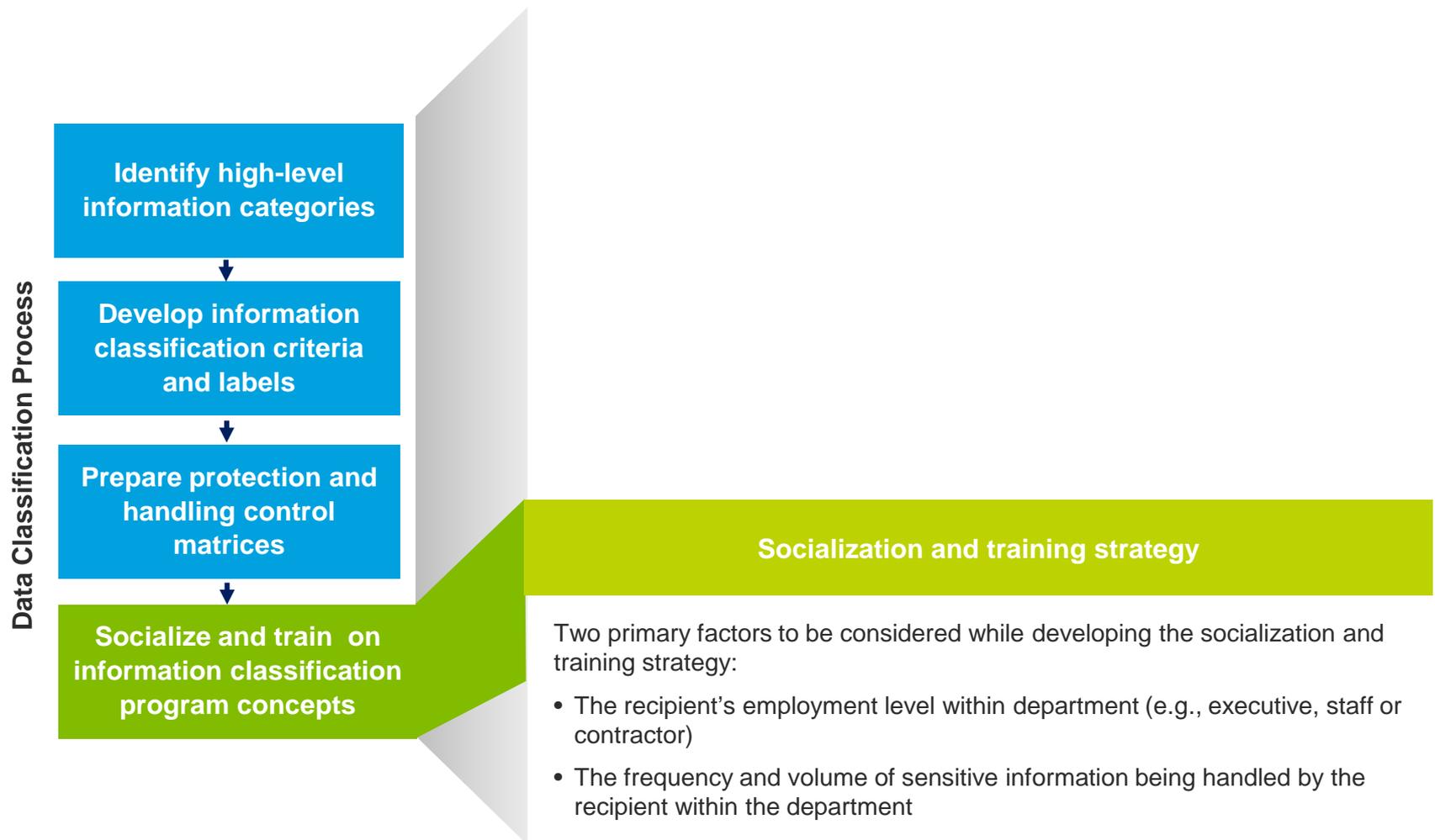
Data classification process

Step 3: Protection and handling control matrices



Data classification process

Step 4: Socialize and train users on program concepts



Question & answer

Contact info

Tim Sanouvong

Public Sector (State Government) — Cyber Risk Services

Deloitte & Touche LLP

tsanouvong@deloitte.com



Connect with me on LinkedIn

Swapn Arora

Cyber Risk Services

Deloitte & Touche LLP

swarora@deloitte.com

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.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see 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.
36 USC 220506
Member of Deloitte Touche Tohmatsu Limited



Future ISOAG

December 2, 1:00 - 4:00 pm @ CESC
Speaker: Mike Snodgrass

ISOAG meets the 1st Wednesday of each month in 2015

ADJOURN

THANK YOU FOR ATTENDING

