dito

Digital Transformation Journey

Re-Imagining CyberSecurity as a Benefit

Adapting security practices within a disruptive digital technology environment

Richard Foltak
Dito CISO, Google Premier Partner

Table of Contents

01 Understanding Our New Reality

02 CyberSecurity Requirements are Changing

03 Lead, Follow, or Get Out of the Way

04 Q&A

Understanding Our New Reality

01

Digital Technology is Changing the World

Business Models are changing

Focus changing from product to consumer experience

Role of Technology Leaders are changing

Technology doesn’t just support the business, it is an integral part!

We don’t do technology for technology’s sake

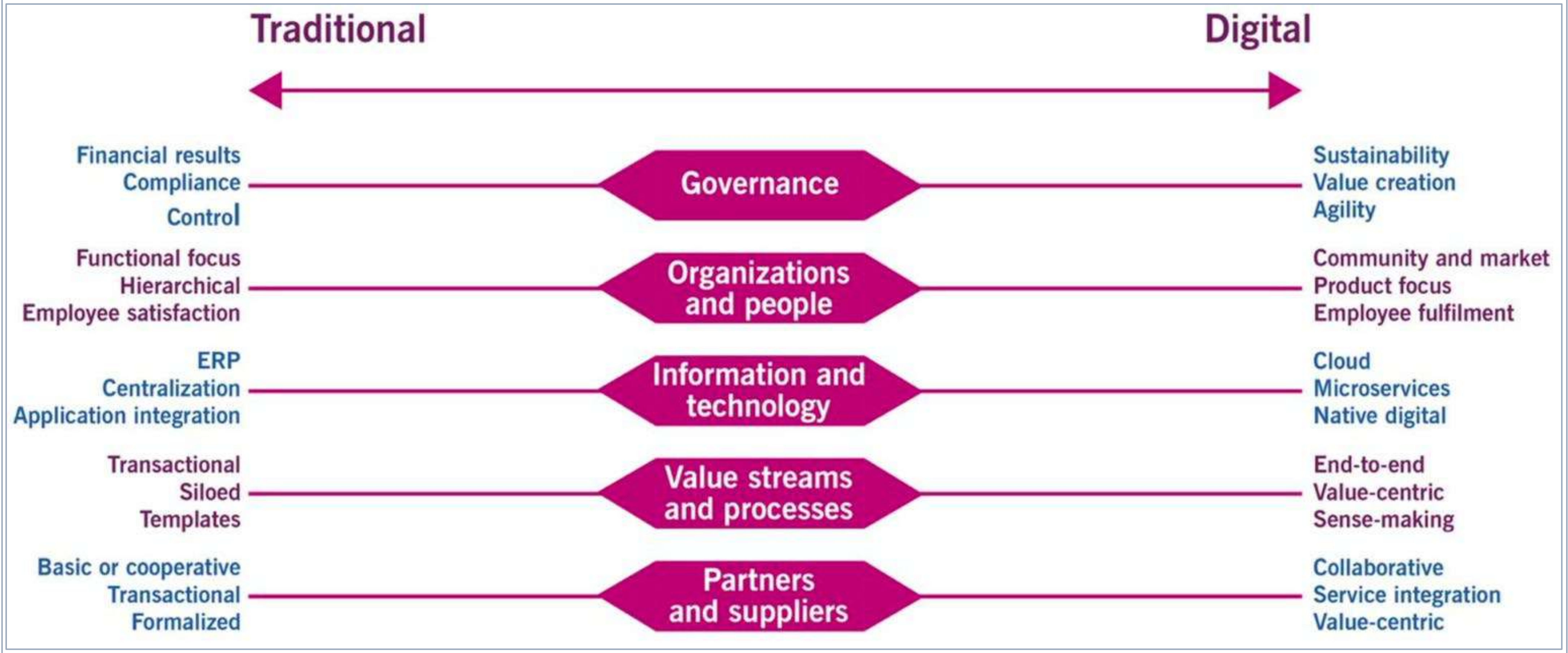
Accelerated Innovation

Increase in urgency for organizations to change and adapt

Hypercompetitive environment - you no longer have the luxury to ignore your place in the environment

What type of Organization are you?

Digital Transformation and IT Strategy



Traditional		Digital
Financial results Compliance Control	Governance	Sustainability Value creation Agility
Functional focus Hierarchical Employee satisfaction	Organizations and people	Community and market Product focus Employee fulfilment
ERP Centralization Application integration	Information and technology	Cloud Microservices Native digital
Transactional Siloed Templates	Value streams and processes	End-to-end Value-centric Sense-making
Basic or cooperative Transactional Formalized	Partners and suppliers	Collaborative Service integration Value-centric

* *ITIL Leader- Digital and IT Strategy*

ITIL provides a set of interrelated best practices that provide guidance for developing, delivering, and managing enterprise IT services

Story Telling Time

Why The Urgency?

verizon

The Cycle Time Problem

In 2017, it used to take 12-18 months to build a new application from start to finish

In 2017, it required 9-12 months to design, order, wait, setup and operationalize new hardware in data center

New innovative platforms have emerged that radically change the new application turnaround time: 18 months ->6 days!

Still takes 9 - 12 months to deploy your own hardware in a data center

Speed allow leaders to fail fast!

This experience led Verizon to embrace Public Clouds

No more waiting for infrastructure

Changing of the guard

If leaders can't adapt, they are being replaced

NEW YORK STATE

COVID-19 Vaccine Scheduler

Not just private enterprises need to respond quickly

Governments are under increasing pressure to deliver services to their stakeholders quickly and with the same quality as leading enterprises

When governments fail to deliver - Front page news

NY State avoided the wall of shame

Ability to quickly respond to new needs

NY State delivered a water utility assistance app in under 2 months

Deloitte.

Resistance is Futile!

Seen many Fortune 1000 leaders replaced for not having a Digital Transformation plan by the board of directors

CISOs who can't adapt… are being forced out

Culture eats strategy for breakfast!

Security teams enjoy their silos and are naturally resistant to change

Security practitioners have a natural "hesitancy" toward automation

Shortage of skilled cybersecurity talent - only getting worse

Security teams are seen as the biggest impediments

Tend to focus on technology solutions rather than security principles

The Innovation Cycle -> Faster Outcomes

Innovate

Innovation changes current situation. Often, initially not very reliable. Can provide competitive advantage to early adopters

Operate

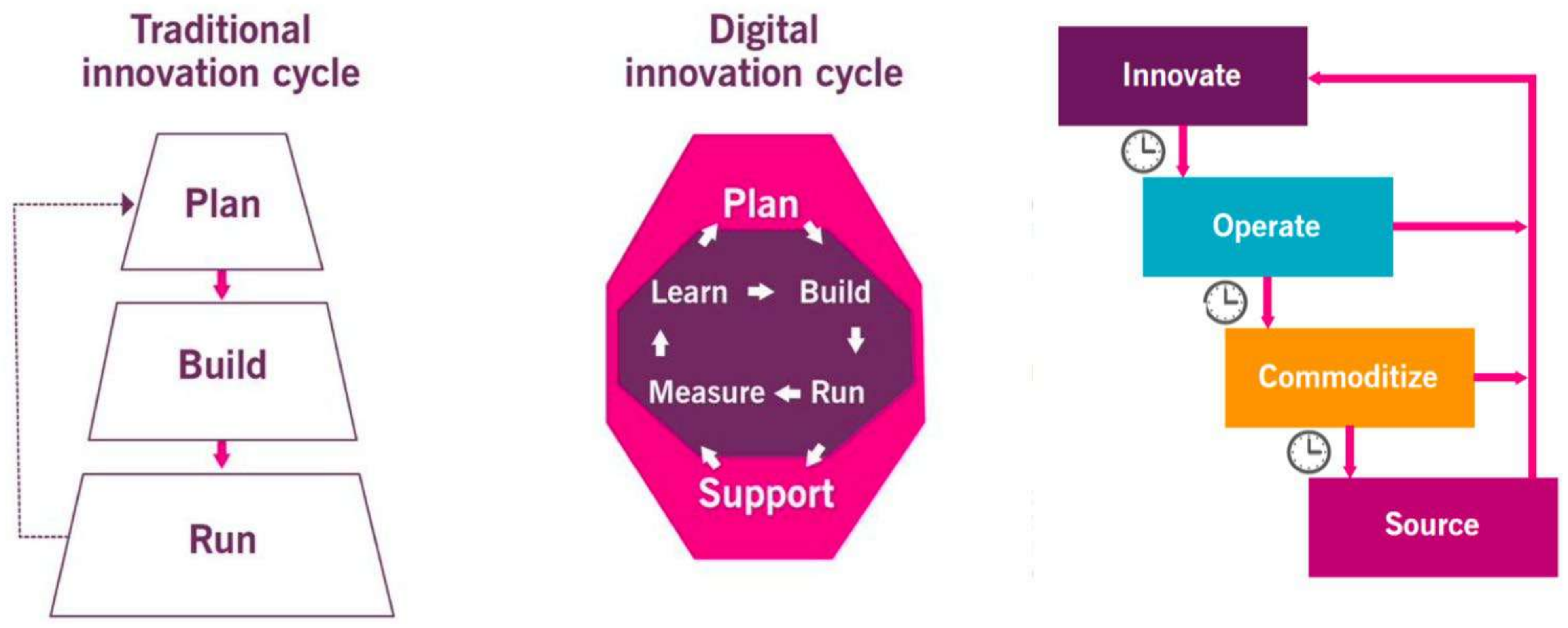
Organizations use standard processes to produce consistent, predictable results. Becomes standard business operation quickly

Commoditize

Other organizations begin to use and replicate innovation. No longer unique of competitive advantage, essential to stay in business

Source

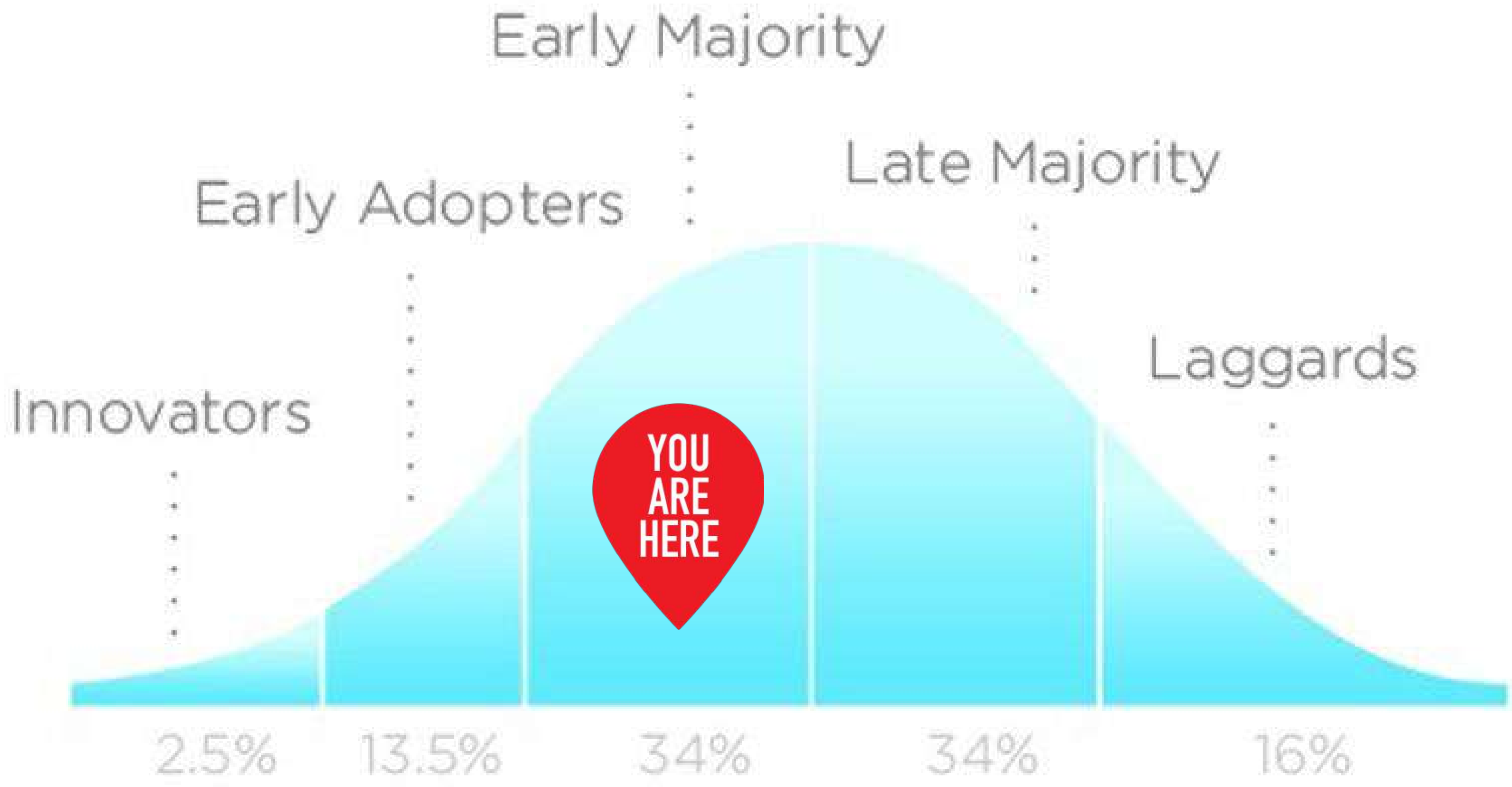
Commoditized technology becomes inexpensive. Skills become abundant. Outsourcing becomes common.



ITIL Leader- Digital and IT Strategy

Security teams need to adapt or risk being left out of the conversation

Innovation Adoption Lifecycle - Digital Transformation



INNOVATION ADOPTION LIFECYCLE

CyberSecurity Requirements are Changing

02

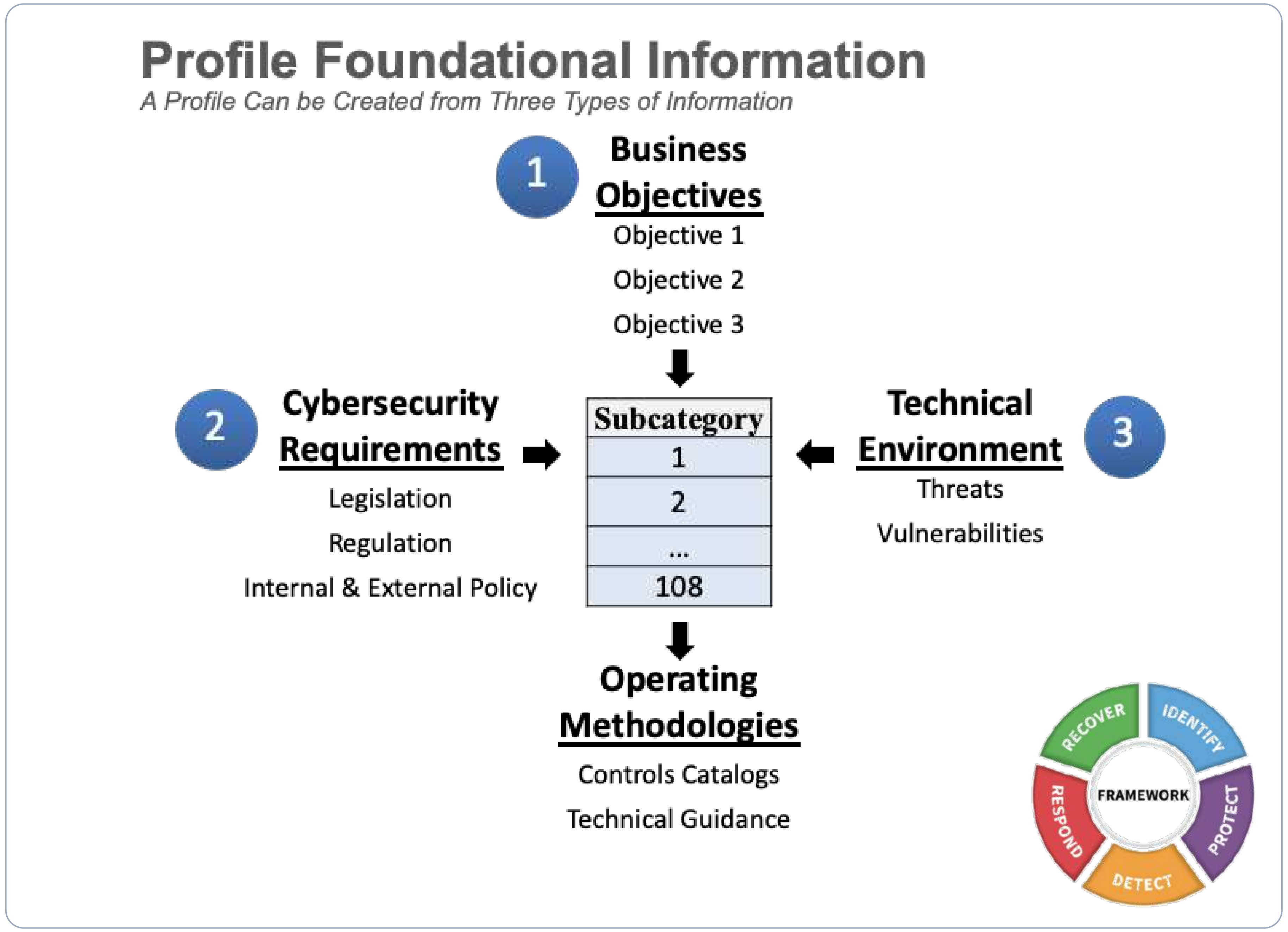
The Role of CyberSecurity

NIST 800-53

Catalog of controls that supports the development of secure and resilient information systems. These controls are operational, technical and management (People, Processes, Technology) safeguards that when used maintain the confidentiality, integrity and availability (CIA triad) of information systems

(CM-6): Achieve the most restrictive implementation of an information system that realizes an organization's **business objectives**

NOTE: CyberSecurity is there to enable the business objectives!



Profile Foundational Information

A Profile Can be Created from Three Types of Information

1 Business Objectives

Objective 1

Objective 2

Objective 3

2 Cybersecurity Requirements

Legislation

Regulation

Internal & External Policy

Subcategory
1
2
...
108

3 Technical Environment

Threats

Vulnerabilities

Operating Methodologies

Controls Catalogs

Technical Guidance

Let’s Summarize The Challenges

Attack Vectors growing at every layer

Threats are growing against every layer of the IT stack

CyberSecurity Talent Shortages

Insufficient security talent available to cover existing IT needs

IT landscape is growing, driving skill updates… and expansion

New technologies require new security skills: How can you secure technologies you don’t even understand? IOT, AI/ML, Data hyper-expansion, etc.

Regulatory Requirements are getting Stricter

GDPR, CCPA, OCC, etc.

Significant existing Technical Debt

Many Organizations lack basic maturity with existing infra

Cost of Breach going Up

Reputational risk can be as bad as a breach

Budgets are not growing

Everyone is being asked to do more with less

Yet…

CISOs are still supposed to protect their organization with due diligence and due care. Just way faster and with less resources…

Lead, Follow or Get Out of the Way

03

Multiple options available…

Lead

Embrace the latest technological advances as part of your digital strategy and work with new ecosystem leaders in helping in your digital transformation journey.

There are many areas where your business could significantly benefit from taking a leadership role using newer technologies that are built to deliver value.

Follow

You don’t have to lead when you can just follow what someone else implemented.

The new digital ecosystem leverages automation to standardize product and service delivery. This enforces compliance to the highest security requirements within industries.

Why be the leader when you can quickly follow?

Get Out of the Way

Organizations are outsourcing IT services (including application modernization and maintenance) to 3rd parties that can deliver change enablement better and faster than their current IT.

Many 3rd parties have economies of scale and very skilled talent with deep technical expertise.

If You Lead or Follow ->Get Good at Automation

Infrastructure as Code

Immutable infrastructure is a security benefit. Everything is guaranteed to be build to your strict standard. Prevent deviations by version controlling your infrastructure.

DevSecOps

DevOps is the merger of Development and Operations. Most organizations have included Security into the model to effectively operate as DevSecOps. Existing tools exist to allow teams to move quickly, and securely.

Security Automation

Automating security best practices is a must. Stop a la carte configuration. There is no reason why any deployment is a SnowFlake. Set yourself on a few secure choices and harden those to the max.

Automated Remediation

SOAR (Security Orchestration, Automation, and Response) can significantly improve SOC team responsiveness.

Automated Compliance

Change Management and Automated Compliance reports are possible in an API driven environment. Enforce compliance by removing the humans to just “break glass”.

Medium Investment -> Big Rewards

Automation does not come for free. But, incorporating security into your automated standardize deliverables will keep paying dividends and allows you to move at the speed of software.

Let's get Tactical

Innovator Examples

Chase Bank

Jenkins (CI/CD)

Immutable Infrastructure
No VM lives longer than 2 weeks
Everything is created from base

No patching…
Lower operating costs
More secure

Apple

Puppet/Chef

All Cisco Networking Equipment
All CPUs, Storage, etc…
Source of Truth is "git" for config

No config drift on premises or in the cloud

Verizon

Ansible

All Palo Altos and Checkpoint FW
All Netscaler, F5 and AVI LB/WAFs

All resources are created / destroyed via application enablement web app or API

Standardized app deployments almost instantaneous

Amgen

AWS Lambda

Purchase AWS Commit resources automatically
Auto shutdown resources when off hours

Automated process by running financial reports weekly to dynamically commit EC2 resources based on usage patterns

Tagged resources on usage to automatically turn them on/off

Q&A

04