PP&CO ALLIANT CYBERSECURITY

CPRA and Data Privacy Changes

What your business needs to know to stay afloat

Who We Are

Alliant Cybersecurity is an information security subsidiary of

alliantgroup®

SOC 2 TYPE 2
AICPA SOC

2021 Inc. BEST WORKPLACES

Privacy Shield
Compliant

GENERAL DATA PROTECTION REGULATION
★★★★★
GDPR
READY

2001
Founded

900+
Employees

18,000+
Customers

ALLIANT
CYBERSECURITY

Rick
Lazio

Rick Lazio is a former U.S. Representative from New York serving in Congress from 1993-2001. While there, he became a strong advocate for small businesses by sponsoring the successful Small Business Tax Fairness Act. After Congress, Rick moved to the private sector working for JP Morgan Chase as a Managing Director and then Executive Vice President.

Rick is committed to his continued interest and support of small to mid-sized businesses by brokering his insight and experience in the public and private sectors to provide strong incentives for job growth.

Kelly Onyedebelu

Kelly is Alliant Cybersecurity's lead Cybersecurity Solutions Associate. With experience in the oil and gas industry, health care, government, and enterprise, Kelly understands the inner-workings of cybersecurity and its implementation in a way that leaves positive impressions on all of Alliant’s clients.

Kelly holds a number of certifications in cybersecurity, project management, and governance. He has worked for over a decade to provide advisory services and implementation guidance to customers from all walks of life. This knowledge, coupled with his customer service experience, has allowed him to make an impact throughout all stages of the business.

ALLIANT
CYBERSECURITY

What is the current state of affairs?

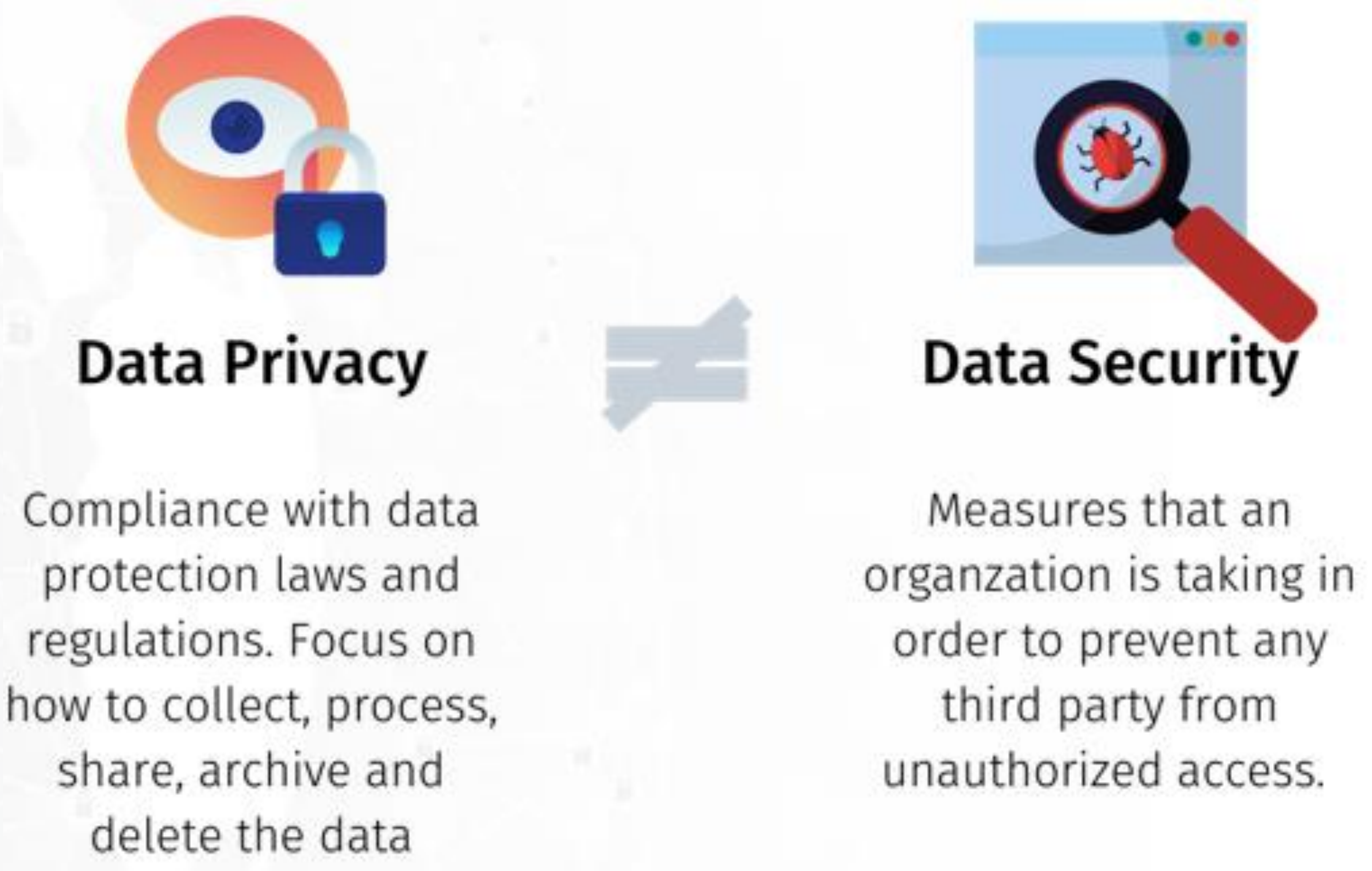
The need for Cyber Hygiene

Cyber hygiene helps reduce those vulnerabilities by identifying risks and deploying mechanisms and strategies to reduce or resolve them. By practicing cyber hygiene, organizations strengthen their security posture and can more effectively defend themselves against devastating breaches.

The need for Data Privacy

Keeping private data and sensitive information safe is paramount. The lack of access control regarding personal information can put individuals at risk for fraud and identity theft. Additionally, a data breach at the government level may risk the security of entire countries.

Data Privacy and Data Security, although not necessarily the same, are both equal components in ensuring that your business is compliant with the CCPA



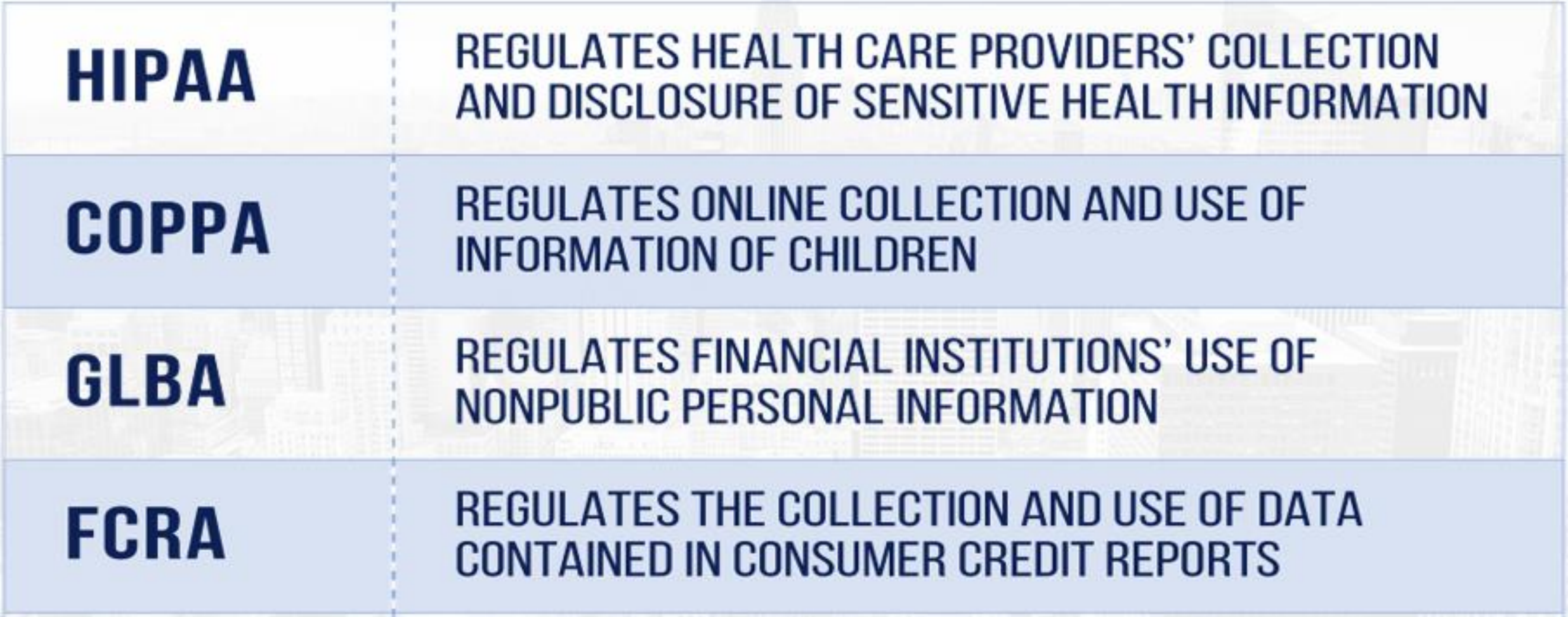
Data Privacy ≠ **Data Security**

Compliance with data protection laws and regulations. Focus on how to collect, process, share, archive and delete the data

Measures that an organzation is taking in order to prevent any third party from unauthorized access.

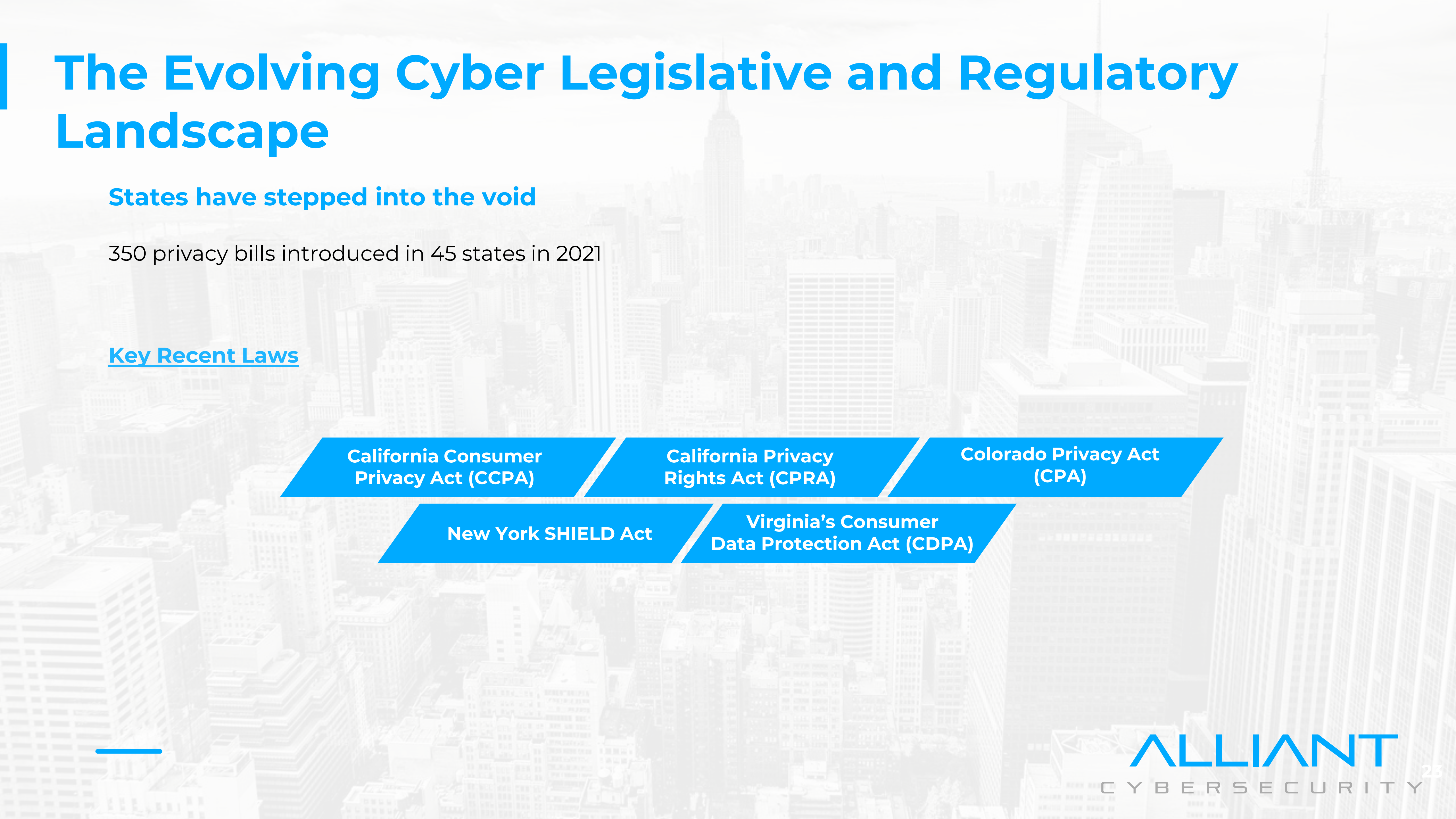
ALLIANT CYBERSECURITY

Current American Data Privacy Policies



HIPAA	REGULATES HEALTH CARE PROVIDERS' COLLECTION AND DISCLOSURE OF SENSITIVE HEALTH INFORMATION
COPPA	REGULATES ONLINE COLLECTION AND USE OF INFORMATION OF CHILDREN
GLBA	REGULATES FINANCIAL INSTITUTIONS' USE OF NONPUBLIC PERSONAL INFORMATION
FCRA	REGULATES THE COLLECTION AND USE OF DATA CONTAINED IN CONSUMER CREDIT REPORTS

The Evolving Cyber Legislative and Regulatory Landscape



States have stepped into the void

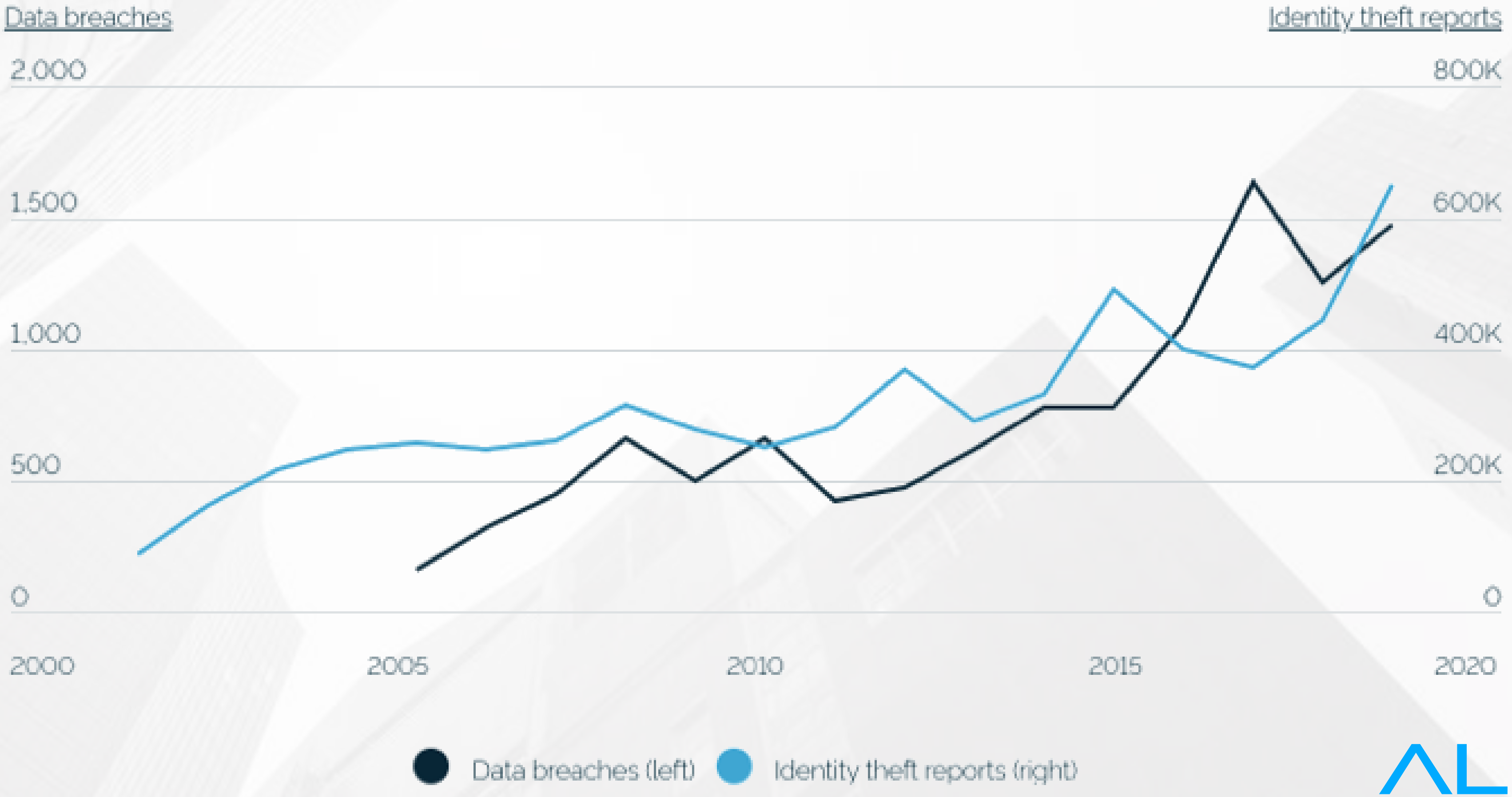
350 privacy bills introduced in 45 states in 2021

Key Recent Laws

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Colorado Privacy Act (CPA)
- New York SHIELD Act
- Virginia's Consumer Data Protection Act (CDPA)

Why Now?

Data Breaches and Identity Theft Reports Have Doubled Over the Past Five Years



Source: Identity Theft Resource Center, Federal Trade Commission's Consumer Sentinel Network Data Book

ALLIANT

CYBERSECURITY

What is the CCPA, the CPRA, and the Differences?

What is the CCPA

The California Consumer Privacy Act (CCPA) is a state statute that was meant to enhance privacy rights and consumer protection standards in California.

ALLIANT CYBERSECURITY

What is the CPRA

In November of 2020, California voters passed the CPRA. The California Privacy Rights Act (CPRA) amends the CCPA and expands its capabilities. With the CPRA, California has established a foundation for consumer privacy regulations.

Functioning as CCPA version 2.0, data and privacy rights will be strengthened.

As it currently stands, the CPRA will take effect on January 1st, 2023!

CPRA Affected Parties

If you are doing business in California and satisfy one or more of the following, your business will be required to adhere to the CPRA:

- Does your business have gross revenue of more than $25 million
- Does your business derive more than 50% of their annual income from the sale of California consumer info
- Does your business buy, sell, share, or collect the personal info of more than 100,000 California consumers annually

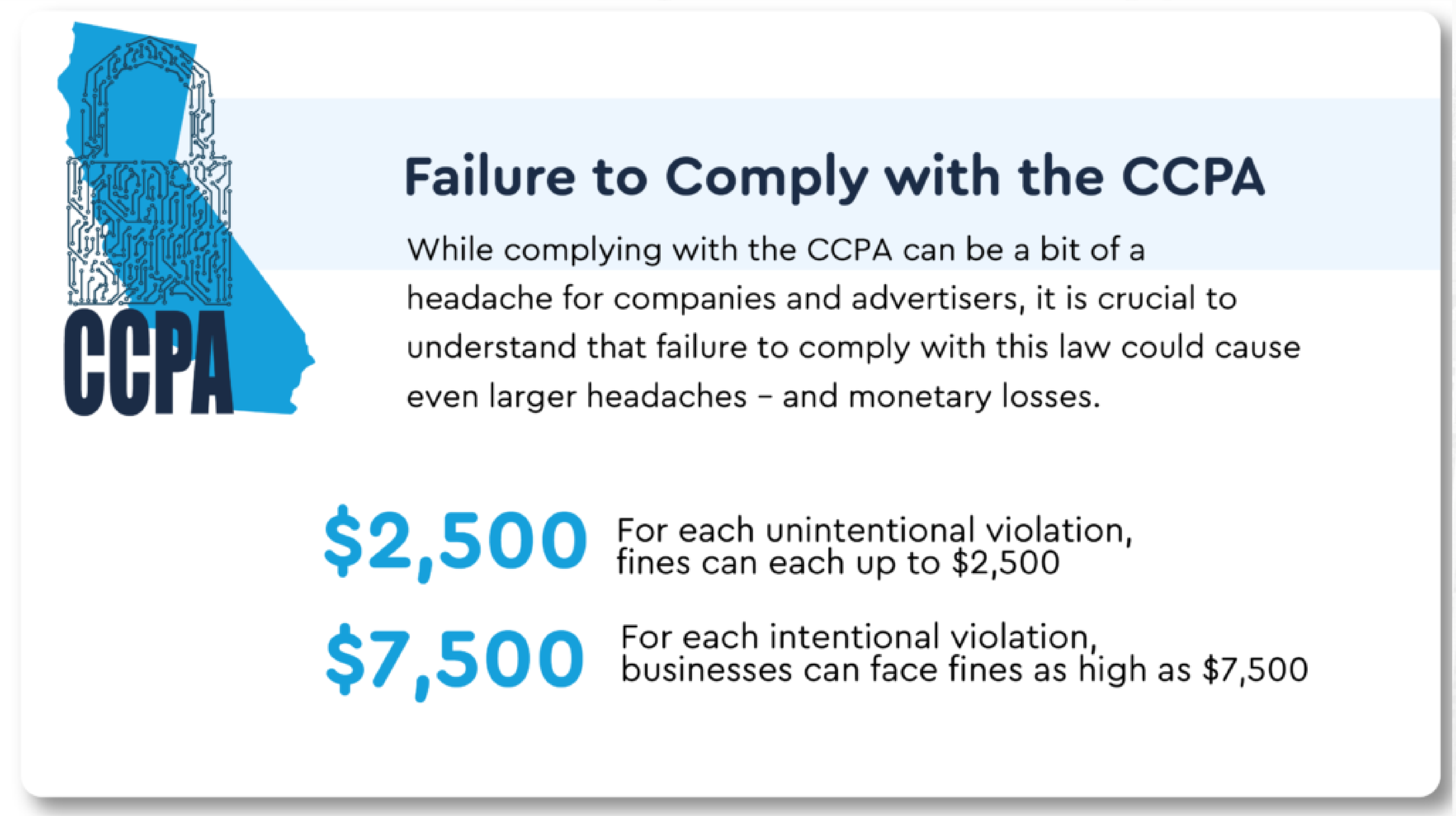
100,000 Consumers

More companies may fall satisfy the third requirement than they may think.

- How many personal records are collected by the business from user intake, sales leads, or are purchased from a data broker?
- How many website visitors do you get annually? Does your website use cookies?
- If your business uses a customer relationship management tool, how many contacts do you have?
- How many unique emails accounts are subscribed to your marketing?

ALLIANT CYBERSECURITY

CCPA & CPRA Penalties



CCPA

Failure to Comply with the CCPA

While complying with the CCPA can be a bit of a headache for companies and advertisers, it is crucial to understand that failure to comply with this law could cause even larger headaches – and monetary losses.

$2,500	For each unintentional violation, fines can each up to $2,500
$7,500	For each intentional violation, businesses can face fines as high as $7,500

Which CPRA requirements does your company meet?

A. Gross revenue of more than $25 million?
B. 50% of your annual income comes from the sale of California consumer info?
C. Buy, sell, share, or collect the personal info of more than 100,000 California consumers a year?
D. None of the Above

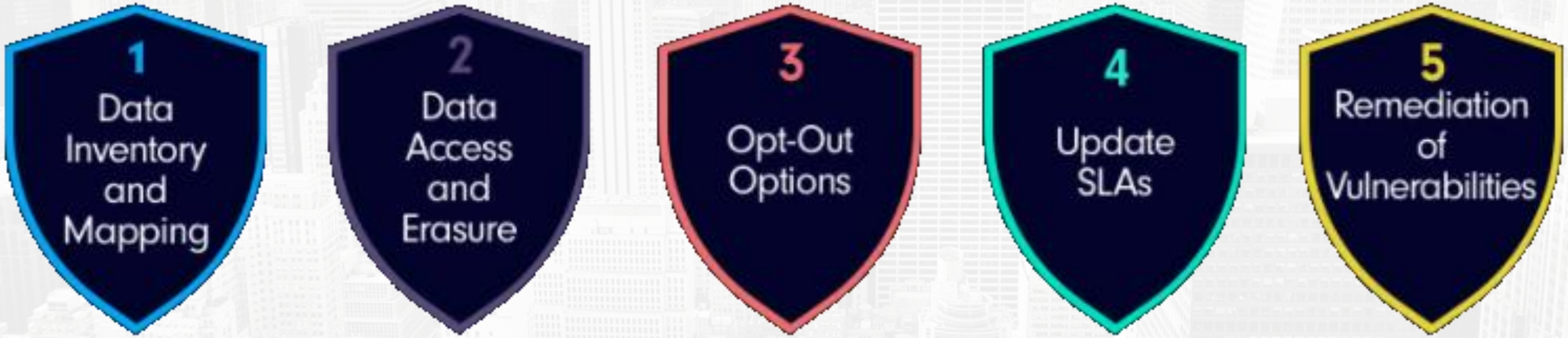
ALLIANT

CYBERSECURITY

ALLIANT
CYBERSECURITY

What should I do next?

The First Steps to Compliance



1 Data Inventory and Mapping

2 Data Access and Erasure

3 Opt-Out Options

4 Update SLAs

5 Remediation of Vulnerabilities

Data Inventory and Mapping

What type of data resides in the environment? Data could be paper data in a filing cabinet or digital data. Do you email information internally? Is information downloaded onto your users' computers? Understanding where this data resides and where it is stored is important.

Take the opportunity to build a data map. That way, it is easy to understand where data resides. Your organization will be in a better position to secure this data once the mapping is complete.

ALLIANT
CYBERSECURITY

Data Access and Erasure

Once an understanding has been made regarding where data resides, it is important to understand who has access to that data. Are you able to determine if data is accessed, transmitted, or erased? Can you identify if a breach has happened in your environment?

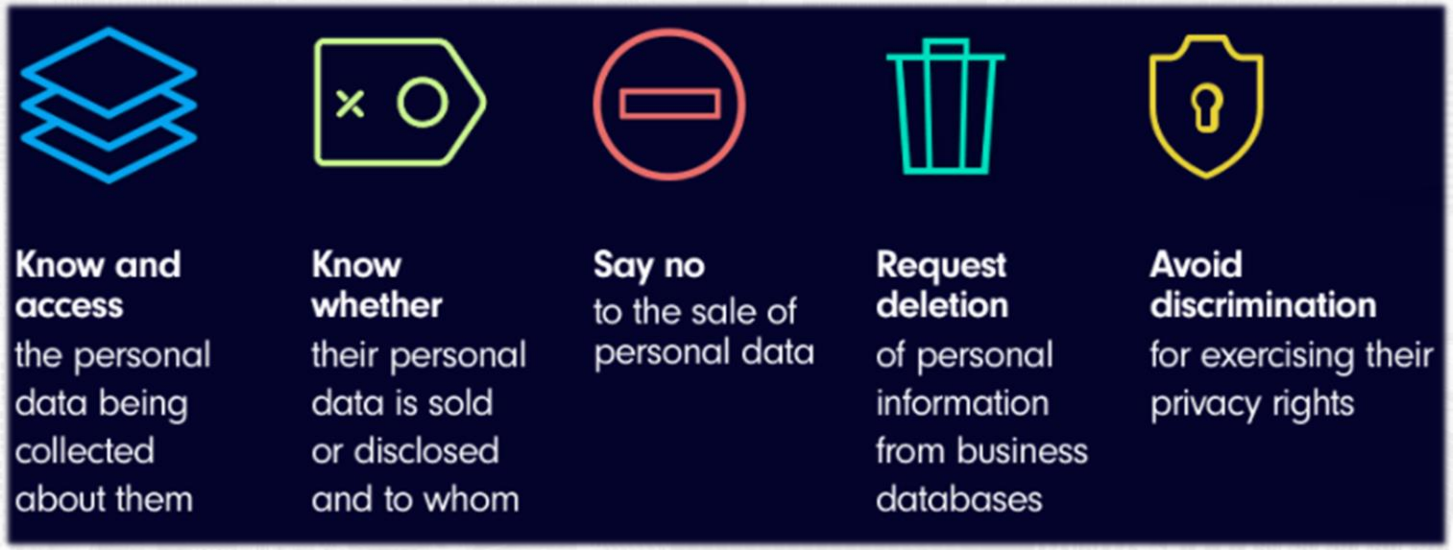
ALLIANT
CYBERSECURITY

Opt-Out Options

Privacy is of the utmost importance. For that reason, it is important to construct a privacy policy that matches your specific CPRA requirements.

Your privacy policy should be reviewed annually and adjusted as needed.

The privacy policy should include information regarding the following:



Know and access the personal data being collected about them

Know whether their personal data is sold or disclosed and to whom

Say no to the sale of personal data

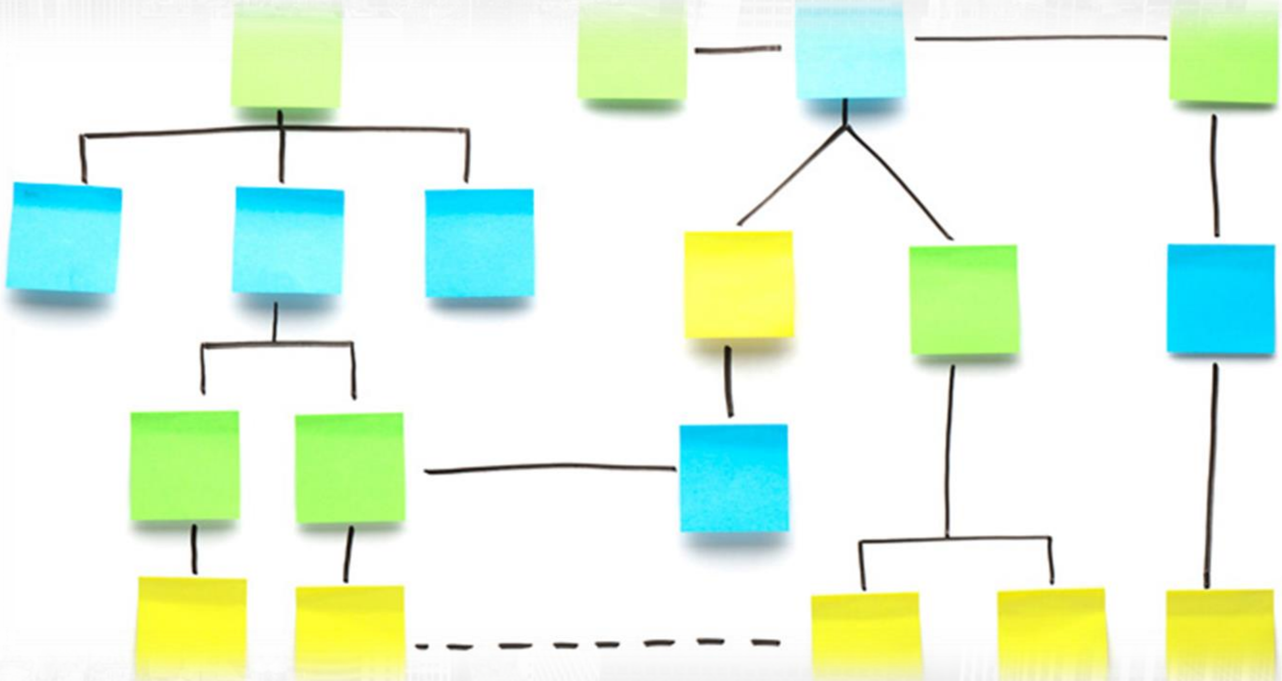
Request deletion of personal information from business databases

Avoid discrimination for exercising their privacy rights

Workflows and Process

It is important to have documented Service Level Agreements in place so that there is a clear understanding of vendor responsibilities and internal responsibilities of the business in the event of a breach. Employees and vendors should understand what to do during a breach including determining the breadth of the breach, when to act, and how breach notifications should take place.

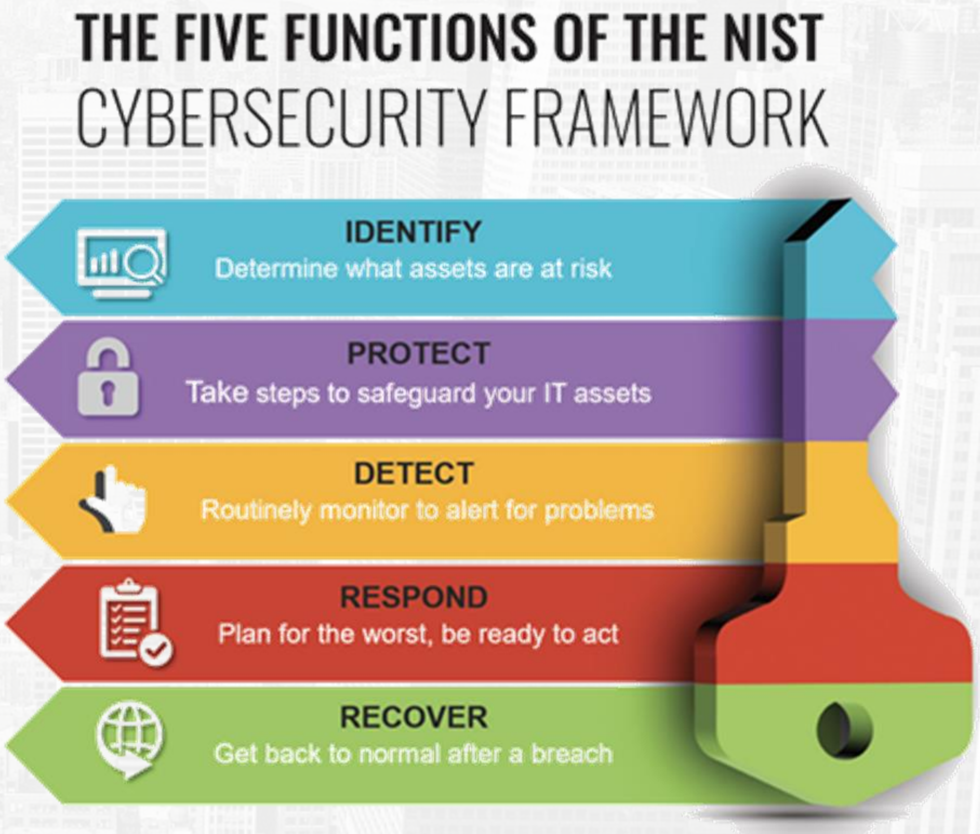
Keep in mind, breaches that can impact more than 500 people must be reported to the state!



ALLIANT
CYBERSECURITY

Implement a Vulnerability Management Program

A vulnerability management program should be implemented in the environment. Such a program allows for vulnerabilities to be identified and assests protected in the enterprise. Without a program in place, your business could fall victim to the very vulnerabilities that bad actors look for when infiltrating systems.



THE FIVE FUNCTIONS OF THE NIST CYBERSECURITY FRAMEWORK

IDENTIFY
Determine what assets are at risk

PROTECT
Take steps to safeguard your IT assets

DETECT
Routinely monitor to alert for problems

RESPOND
Plan for the worst, be ready to act

RECOVER
Get back to normal after a breach

Which resolutions would be most difficult to achieve in your environment?

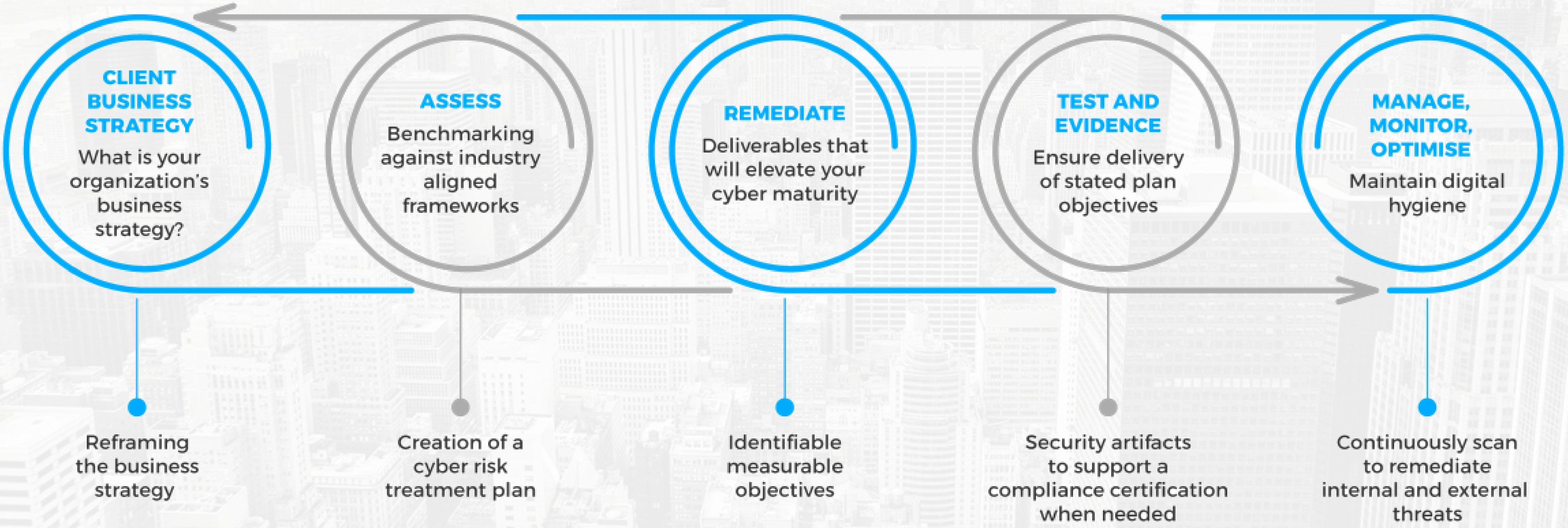
A. Determining where data actually resides?
B. Understanding who is interacting with your data?
C. Do you have a privacy policy in place?
D. Do you have an internal plan for handling a breach?
E. How are you detecting the vulnerabilities in your environment

ALLIANT
CYBERSECURITY

ALLIANT
CYBERSECURITY

What should I do next?

Perform a **Risk Assessment**



CLIENT BUSINESS STRATEGY

What is your organization's business strategy?

Reframing the business strategy

ASSESS

Benchmarking against industry aligned frameworks

Creation of a cyber risk treatment plan

REMEDIATE

Deliverables that will elevate your cyber maturity

Identifiable measurable objectives

TEST AND EVIDENCE

Ensure delivery of stated plan objectives

Security artifacts to support a compliance certification when needed

MANAGE, MONITOR, OPTIMISE

Maintain digital hygiene

Continuously scan to remediate internal and external threats

ALLIANT
CYBERSECURITY

How We Help

- Controls and Policy Planning
- Advisory Services
- Managed Security Services
- Cyber Reviews & Assessments
- Offensive Penetration Testing
- Breach Response & Digital Forensics

ALLIANT
CYBERSECURITY

Questions?

ALLIANT

CYBERSECURITY

PP&CO

ALLIANT

CYBERSECURITY

THANK YOU