Regulation Means Change

TONY GONZALEZ

DIVISIONAL INFORMATION SECURITY OFFICER, QBE NORTH AMERICA

Impact of Regulations Discussion

- *Regulations Mean Change*
- More complex regulations, such as the General Data Protection Regulation (GDPR), have come into play due to the rise of data breaches forces. As data today is viewed as a such an asset, it is also a tremendous liability. Understanding that, organizations must consider both while they implement technologies that will be both innovative their business, but also cost effective.
- Takeaways:
- Understand the latest regulations, such as GDPR
- How to tell your CEO and other business stakeholders that data protection can be a key differentiator for your organization
- The steps needed to take to be regulatory compliant

Understanding the Impact of Current Technology Trends

- What data we use and how we use it is changing constantly
- Data Analytics and the Digital boom drives us to want to know everything about everything and anyone
- Cloud computing where all our data is in remote hosted facilities and shared and transmitted through our complex ecosystem is now considered the norm
- Understanding user behavior and having strong data governance capabilities is growing in importance
- Businesses and their IT organizations need to consider their multi-national customers, and where they host their data in-order to accurately assess their regulatory obligations.
- Discussions are already happening to understand how regulations will apply to consumers with multiple citizenship.

Regulations are a Gift

- Our chance to turn lemons into lemonade
- We are all talking about GDPR, WHY?
  - GDPR contains strick consequences for non-compliance
    - Fines up to 4% of global revenue
  - Consumer awareness and concern over who has their data and how it is used
    - Breaches carry even more impact on the reputational damage of an organization
  - Executives are concerned about the ability to withstand extensive reviews by regulators
  - All regulations have the capability to impact us based on our customers perception of us or direct impact to our bottom line
  - This is the opportunity to gain support to do what is needed

GDPR Requirements

Requirements in a nutshell

Ensure we only collect the minimum personal data needed, we only hold it for as long as necessary, and consent is in place if required

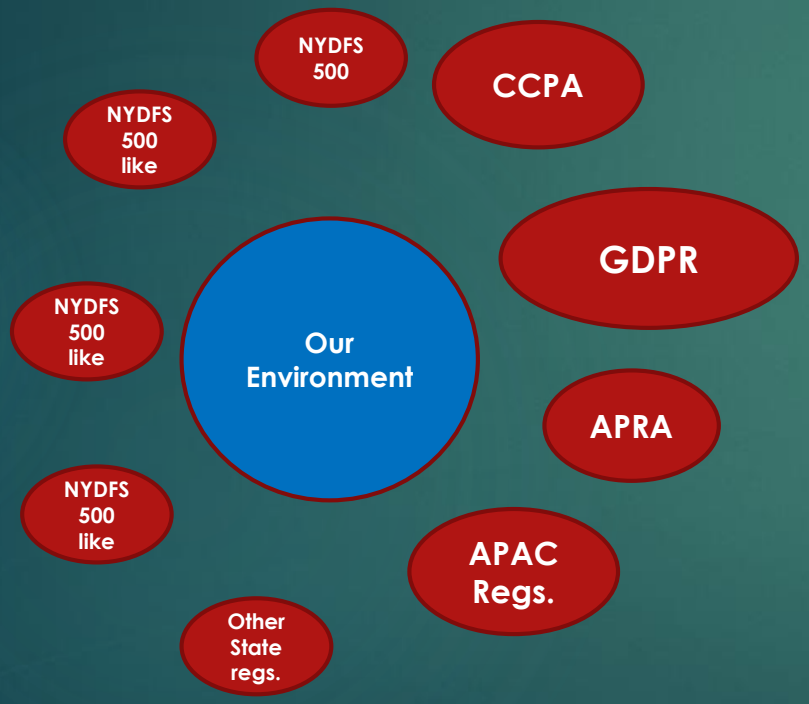
Ensure we understand personal data flowing into, through and out of an organization to ensure personal data is secure, handled with care and accessed appropriately.

Ensure processes are in place to respond to any customer requests, such as a request to delete their data - known as the 'right to be forgotten'

Ensure that any personal data breaches are reported to the Information Commissioner, within a new 72-hour deadline

Have evidence, monitoring and oversight in place to ensure ongoing compliance

Having a Global Regulatory Perspective



- NYDFS 500 was one of the first regulations to explicitly call for the use of specific technologies
  - encryption at rest and in transit
  - Multi-factor Authentication(MFA)
  - There are several states that have followed with adoption of similar regulations
- GDPR introduced the concept of "Right to Be Forgotten"
  - Consumer right to request to see what data we have of theirs
  - Companies needing a mechanism to produce such data
  - Consumer having the right to request erasure of all their data
  - Inability to comply could evoke heavy fines from regulators
- APRA just releases an addendum that requires cloud solutions to be considered outsourcing
  - All outsourcing engagements require regulator notification
- California Consumer Privacy Act(CCPA) follows GDPR requirements less the fine structure
  - Follows GDPR with "Right To Be Forgotten" requirements
  - Allows consumers to file suite if companies cannot comply
  - Other states looking at following California down this path

Stakeholder Awareness

- Having open dialogue with key stakeholders and C-suite executives is crucial to any successful Compliance and Security program:
  - Make the conversation a business conversation not a technical one
  - Take the time to educate and make stakeholders aware how your program will address compliance and achieve success
  - Drive the conversation from what value the program brings
    - Having a strong compliance and security program is a business enabler that allows innovation and creativity to prosper with lower associated risk.
  - In most organizations technology is a key differentiator that makes one organization more attractive to consumers than others
    - Your program can be the catalyst to your organizations success

Successful Compliance Programs

- Understanding your regulatory landscape
  - Build a "greatest common denominator approach" to develop requirements
- Privacy Compliance and Security go hand in hand
  - Ensure Security basics and best practices are in place and functioning through:
    - Secure coding and integrated security SDLC practices
    - Strong Data Loss Prevention(DLP) capability
    - Strong training and awareness programs
    - Continuous improvement and frequent risk based assessments
- Implement an effective 3rd Party Vendor Governance and Assessment Program
- Implement a Data Governance program to manage data effectively
  - Implement effective data retention policies
- Don't treat compliance as a project
  - Make sure there is an organization and funding to build a sustainable compliance capability

Thank you
?