Regulatory Framework: Putting data privacy and protection at the centre of your business

At the centre of any great art you find people. It’s the same with data privacy and protection.

Why do we need regulatory frameworks?

There are some key reasons why regulatory frameworks are needed:

1. **GDPR**: In 2018, the General Data Protection Regulation (GDPR) came into effect in the EU, imposing strict data protection regulations on organizations across the region.
2. **CCPA**: The California Consumer Privacy Act (CCPA) was enacted in 2018, giving California residents greater control over their personal data.
3. **PDPA**: The Personal Data Protection Act 2018 in Thailand was introduced to protect personal data.
4. **PIPEDA**: The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada defines how private information is to be handled.
5. **Notifiable Data Breaches Act 2017**: In Australia, this act requires organizations to notify data breaches.

These regulations are designed to protect individuals' rights to privacy and prevent organizations from misusing personal data.

The Benefits of Frameworks:

- **40%** of organizations benefit from having strong frameworks in place.
- **47%** of organizations report an increase in customer trust.
- **73%** of organizations believe that GDPR has had a beneficial impact on consumer trust.

The Issues in Compliance:

- **10%** of all companies are complying with data protection regulations.
- **97%** of companies are not fully compliant with data protection regulations.
- **24%** of organizations said it would take more than a year to get GDPR ready.

Cyber Resilience:

- **60%** of data breaches can be prevented by simply following best practices.
- **66%** of organizations have at least 90% of their cyber resilience plan in place.
- **24%** of organizations have no cyber resilience plan in place.

How can you approach data privacy whilst complying with regulatory frameworks?

Micro Focus provide an end-to-end solution encompassing all 3 vital pillars of data privacy and protection.

1. **FIND AND ANALYZE**
   - Identify and assess risks to data.
   - Implement controls to mitigate risks.

2. **STORE AND APPLY POLICY**
   - Apply and enforce policies across the organization.
   - Ensure compliance with regulatory frameworks.

3. **SECURE AND ENCRYPT**
   - Protect data at rest and in transit.
   - Encrypt data to ensure confidentiality.

These steps help organizations to comply with regulatory frameworks while protecting the integrity and confidentiality of their data.

Regulations to take into account:

- **California’s recently enacted CCPA**
- **India’s Personal Data Protection Bill of 2018**
- **Brazil’s General Data Privacy Law 2018**
- **Turkey’s KVKK**
- **Thailand’s PDPA**
- **Canada’s PIPEDA**
- **Australia’s Notifiable Data Breaches Act 2017**

That’s not to mention industry-specific regulations, such as HIPAA for US healthcare providers.

It’s a complex process. The Issues in Compliance

Non-compliance/compliance issues can exacerbate issues with your organization’s cyber resilience.

- **60,000,000** exposed records in 2019
- **$4 million** The approximate average cost per breach as of 2019, with the US the most expensive country and healthcare the most costly industry.

- 65% of small and medium-sized businesses (SMBs) are out of business within six months of being hit by a cyber-attack and...

- **66%** of SMBs would shut down if hit by a data breach and only...

- **24%** of organizations have C-level buy-in for their cyber resilience plans.

- 60% of US companies are actively working to comply with 50 or more privacy laws.

- **59%** of organizations are currently meeting all GDPR requirements.

- **9%** of organizations said it would take more than a year to get GDPR ready.

- **9%** of consumers seeing benefits at least twice that of their privacy spend.

- **75%** of companies recognized they were realizing benefits such as competitive advantage or investor appeal from their privacy investments.

- **9%** of organizations believed GDPR has had a beneficial impact on consumer trust.

- **66%** of respondents said they have greater trust in companies that use their data as a result of the GDPR.

- **16,000,000** records were exposed in 2019.

- **6%** of US companies are currently working with at least 20 privacy laws.

- **95%** of companies were not fully compliant with data protection regulations.

Contact us at Micro Focus - Voltage