ROBERT FRANCES GROUP
Business Advisors to IT Executives
Jul 2, 2020

Five Potential Out-of-Compliance Areas Due to the “New Normal”

RFG Perspective: Initial business transformations in response to the global pandemic focused on meeting the demands of stay-at-home workforces while addressing fluctuations in customer demands. While large organizations were able to quickly meet these substantive changes in customer demand and accessibility, other aspects may have fallen into non-compliance, including sensitive data and personally identifiable information (PII) protections, data governance, and data residency. To ensure continued operations, many institutions will need to launch re-examinations of the data and its supporting compliance, operational, privacy, and security policies and procedures. Businesses must ensure that appropriate measures are enacted and that they can effectively support ongoing customer, business partner, and governmental requirements.

When the COVID-19 pandemic broke out in March, there was a mad scramble to accommodate the shift in business to a work-from-home (WFH) environment and develop new business models so that there would be minimal disruption of service across many industries worldwide. The exceptions were business that could not support WFH (e.g., the hospitality, restaurant, and travel industries).

Speed was vital to the success of supporting most employees working from home. Unfortunately, given the rapid move to WFH around the world, it is highly likely that this major shift in IT operations has inadvertently resulted in a number of out-of-compliance conditions.

Now that we have made the transition to the New Normal, it is time to re-examine areas where enterprises may be out of compliance in some locations and geographies – or across many geographic regions. We believe that there are five areas that need scrutiny.

The five domains most impacted by the new WFH environments are as follows:

- The digital and physical WFH environment
- Data Center and Cloud
- Governance and controls
- Business continuity
- Risk management

The Digital and Physical WFH Environment

While most organizations allowed staff to work from home prior to the COVID-19 lockdown orders, many business applications – most of them providing access to sensitive data – were not accessible from locations outside a company’s site. In some cases, this was dictated by regulatory requirements (for example, trading in stocks and bonds on behalf of the firm). This was also true of some company-sensitive data and personally identifiable information (PII) related to customers and prospects. (Examples of PII include Social Security numbers and HIPAA-protected medical health data). In recent years, GDPR from Europe and CCPA from California are top examples of important new governmental regulations governing data compliance.

As business managers and IT managers, we face several significant challenges to ensure compliance across-the-board, that supports our corporate data policies and complies with governmental regulations:

One of the first challenges to address is protecting end-user devices that access business applications and data. Now, that these applications and data are available from a company-owned end-user device – or even worse, a personal device that may never be properly wiped clean during usage or upon disposal – it is necessary to lock these devices down properly and to guarantee that they conform to regulatory requirements.

A second challenge involves the usage of these devices. The fact is that employees working from home represent a bigger threat to the organization than those at a company site. Companies must recognize that phishing attacks have ramped up considerably over the past few months and the probability of employees falling prey has increased. Secondly, the insider threat is greater now that disloyal employees no longer need to worry about someone looking over their shoulders and may now undertake malicious activities more freely.

Moreover, Enterprises need to ensure that children, roommates, spouses, significant others, friends and family that have the ability to access the devices are locked out. Experience has shown that others will attempt to access the computer for their own personal business -- and that they may even download unauthorized or undesirable applications onto the device. That action alone might bring along malware that could infect the entire company.

A third challenge involves the issue of physical documents. Companies have committed to protect company-confidential and PII data at all times – and the company is required to know where it is at all times (including digital and physical copies of the data).

Is your company still in compliance? We must take inventory of our applications and data – and determine if we are supporting compliance with all governmental regulations and standards – and with our company's data-protection policies.

Here are some questions to consider: if a person asks to have their personal data deleted, as allowed by law, would that still happen -- and would the company know for sure that the data was protected properly? In general, can the firm guarantee that all physical documents are kept under lock-and-key at all times or that they can be deleted when required? In a WFH environment, how can the firm guarantee that non-employees will not able to see data-protected documents?

Data Center and Cloud

The server side is less complex than chasing down non-compliant end-user devices, but there are new exposures. Many enterprises attempted to address some of the Edge challenges by employing a VDI or Desktop as a Service (DaaS) solution. While this keeps PII data from being stored on the employee's computer, it has its own challenges. VDI and DaaS providers usually locate applications from multiple organizations on the same shared infrastructure. The company needs to ensure that all traffic is encrypted, and that sensitive data is encrypted when stored using an encryption method strong enough to prevent tampering by outsiders. Companies must also make sure that policies are in place that restrict access according to the rules that guide the firm's overall compliance requirements.

Many enterprises have moved business applications to the cloud to gain the added capacity needed to support the WFH environment. When migrating to the cloud, the biggest exposure that companies face is the creation of unintended configuration errors. Now that things are stabilizing, IT staff should go back and ascertain that there are no configuration errors. The second cloud exposure is that of code vulnerabilities. When the code errors were behind the company's data center firewall, the problem was limited. But when business applications are running in the cloud, the problem is magnified. Companies need to make sure that they are using effective static and dynamic code-scanning tools that can constantly monitor and report on the environment and on any new code changes.

Governance and Controls

Governance of user data needs to change, and new policies and controls need to be established. The challenge will be to incorporate all the new protective measures without impacting the employees' ability to perform their jobs. For example, an account lockout policy should be put in place to deter attackers from gaining access. However, failed password attempt limits should not be so low that employees get frustrated from lockouts. Audit teams need to perform access, activity, and configuration audits frequently to limit exposure to compliance issues. Additionally, auditors should review and, if needed, update their continuous automated penetration and attack testing policies and procedures.

Moreover, companies need to look beyond their consultants and employees: they must validate that their outsourcers and supply-chain partners are also in compliance and can attest to it. Lastly, companies must be able to attest to their own compliance and be able to withstand an audit.

Business Continuity

Prior to the COVID-19 lockdown, most companies had their business continuity plans written and tested. But circumstances have significantly changed. Therefore, companies must re-visit their existing business continuity and data-protection plans and procedures as it is no longer just about ensuring a known number of sites can be operational in case they need to move to irregular operations.

The question is whether the business can continue to operate when applications, data, and individuals are dispersed across a myriad of locations, each of which may be working under different local directives. It is important that enterprises not only develop new business continuity plans for the New Normal, but also run tabletop exercises to prove that they will work reliably.

Risk Management

No matter how diligent a company is, its overall risk exposure has not dropped to zero. The key question becomes – as always – what is acceptable risk and how can it be achieved? Some areas to examine are whether the recovery point objectives (RPOs) and recovery time objectives (RTOs) are still practical; whether the decision-making matrix still works; and whether the call trees to reach IT staff and other key stakeholders need updating. In other words, companies must determine whether all logistical obstacles to global compliance policies – clear across the virtual extended organization – have been considered and addressed.

Summary

We are living through a period of tectonic shifts in the world's economy. There is no business-as-usual – and the future is uncertain. However, even the extreme case of dealing with simultaneous health and financial crises should not prevent enterprises from complying with existing data-protection regulations. If there is one certainty, it is that, given enough time, governments will aggressively fine businesses that fail to comply with their regulations – resulting in financial damage to the business and its reputation.

RFG POV: The shift caused by the COVID-19 lockdown to a more digital world for conducting business is not temporary. Rather, it is a New Normal for business, causing an acceleration of digital transformation, application modernization and data-based analytics. Business and IT executives must work together to optimize their new work models – and ensure that they are in full compliance with all appropriate regulations, across all geographic regions worldwide. Each organization must review its compliance situation – and begin addressing critical issues before government agencies, for enforcement purposes, start looking for prominent corporate examples to penalize and publicly embarrass.

Additional relevant research and consulting services are available. Interested readers should contact Client Services to arrange further discussion or interview with Mr. Cal Braunstein, CEO and Executive Director of Research. Jean S. Bozman, President of Cloud Architects Advisors, co-authored this research report.