ROBERT FRANCES GROUP
Business Advisors to IT Executives

Nov. 18, 2020

Summary Insights: Aligning Corporate Risk Posture with New Normal Norms

RFG Perspective: The rapid shift to the COVID-19 era work from home (WFH) office and hybrid multi-cloud environment is forcing CxOs to re-examine their enterprise's risk posture for New Normal work conditions. Business and IT executives will need to assess the appropriate measures needed to align their risk posture, given recent changes to customer, employee, business partner, and governmental relationships and requirements. To be effective, these assessments must address business continuity (BC), regulatory compliance, protection of sensitive data and personally identifiable information (PII), data governance across the hybrid multi-clouds, and data residency policies.

We are living in a brave new world – and we've known that ever since the pandemic emerged in early 2020. The reality is that we are now operating in a borderless multi-cloud/edge work environment that is open to many more security risks than traditional office work environments.

Enterprise executives need to understand the extent of their company's risk exposure if they are to protect it from security breaches, data leaks, and cyber-security attacks. Any of those security issues could damage a company's reputation and brand – and allow corporate data to fall into the wrong hands. That's why business, technical and governance risk postures must be examined, understood, quantified and aligned with acceptable levels of corporate risk.

How Did WFH Impact Security Issues?

Significant changes in business, organizational and technical operations have been necessary to effectively deal with the New Normal environment caused by the COVID-19 crisis. The recent modifications to corporate networks and systems consumed significant time and energy expenditures in order to enable access to corporate applications from employees' homes. But these changes also had the unintended effect of impacting corporate risk postures – creating a new set of WFH-related security issues.

Now is the time for the realignment of risk postures, so that they will more closely conform to previous corporate networking and security standards. The re-alignment process will require discussions among, across, and between business leaders, CSO teams focused on security, and the board of directors about levels of acceptable risk. New directives regarding risk tolerances must be communicated and shared throughout the organization and incorporated into standard operating procedures to safeguard corporate data.

Authenticating end-users and their devices is high on the list of priorities for this realignment process. Companies need to recognize that the world has taken on new dimensions that complicate the process of recognizing the identity or persona associated with the end-user device – and the privacy and security of sensitive data.

RFG 100 Panelists and Insights from Participating RFG 100 Executives

On Oct. 28, 2020, RFG facilitated a videoconference on "Aligning Risk Posture with New Normal Norms." The panelists on the call were:

- David Giambruno, founder, Nucleaus
- Bil Harmer, CISO, SecureAuth
- Ravi Ivaturi, SVP, Citi
- Warren Gedge, CTO, ScriptString
- Jean S. Bozman, President, Cloud Architects LLC

RFG 100 executives and panelists recently discussed the business-critical issue of re-aligning risk postures to address the changes that occurred with the rapid shift to the New Normal last spring. In this research document, we include their reflections on the challenges that are associated with a changed IT and business landscape worldwide.

RFG Analysis

Revisions to operating procedures are underway to close security gaps identified by IT organizations. However, business and IT executives often do not recognize the extent to which the work-from-home (WFH) environments can impact daily operations. Slackened guardrails provide unexpected opportunities for unauthorized access to applications and data. Many of these could expose the enterprise to data loss, regulatory penalties, and reputational damage.

Clearly, many enterprises recognize the security threats posed by WFH – and they are working hard to reduce their risk exposures. However, a number of firms may face a future customer and regulatory backlash if an extended relaxation of guardrails results in successful extractions of large quantities of personally identifiable information (PII) and other sensitive information.

Access Control in a Borderless World

In the New Normal world, corporate networks have become truly borderless. It is impossible to know where the boundaries are. Individuals can obtain access to enterprise applications and data from virtually anywhere. Essentially, companies have to start thinking about defending employee's homes – a formidable task – and other, possible entry points to their corporate network. Ubiquitous Wi-Fi access to networks – even from local coffee-shops near employees' homes – provides limited barriers to entry. The question then becomes: How should an enterprise address access control?

Enterprises need to think about access control more broadly, because it can provide a hard-to-defend entry point into the corporation's network, its applications and its data. That's why it is important to have a complete inventory of all of the people who have rights of access – customers, contractors, employees, and suppliers. But it's also important to consider a range of activities and roles that each individual employee may have. Organizations must be able to quickly onboard or offboard individuals, as well as to modify access rights as individuals change roles within an organization, which has been a major shortcoming for enterprises for decades.

Endpoint security is another aspect to be considered in the New Normal WFH world. Traditionally, most corporations – of all sizes – have operated on the notion that their workforce taps into an on-premises intranet most of the time – with some traffic coming from remote networks. Engineers have designed networks and systems and process based on that set of assumptions. In today's borderless multi-cloud and Edge world, with many more access points and permissions, endpoint security becomes more important than ever before.

Culture and Behavior – Impact on KPIs and KRIs

There is a major effort at a number of companies to understand what people are doing, how they're doing it and creating the appropriate metrics to avoid risk exposure. Two forms of metrics help with this: Key risk indicators (KRIs) to identify potential security risks, and key performance indicators (KPIs) to motivate IT organizations to address them. KRIs surface evidence of increasing risk exposures – helping IT managers to detect security exposures that had gone undetected before.

But how can all of this be accomplished when employees are working from home or at other offsite facilities? They are not in the office – an environment that is well-managed and highly controlled via hardware sensors and security software. One way to go is to pursue a minimally invasive trust-but-verify model of oversight; the other version using a very visible Big Brother approach to monitoring that could impact morale, and in turn, potentially reduce worker productivity.

Creating a set of KPIs that shows where the company's people are working – and what they are doing – is achievable. Two factors influencing the success of having KPIs in place are effective personnel communications – and having sufficient time and money allocated to ensure that new security policies and practices are widely understood, used and enforced.

The RFG100 discussion surfaced some new core metrics, as well. These include: How are individuals changing roles, usages, and locations, and how do their work patterns map to what devices they are using?

Given today's telemetry capabilities, one can determine the geolocation of the user and their device. Furthermore, one can now recognize the velocity of change of geolocation and/or device—enough to determine whether the change is a rational one or whether it represents an attack. These vectors become additional metrics and risk indicators for CxO staff to track and to manage, without creating new issues for employees and their families during a pandemic.

Not only are employees working from home, but so are other family members — and those family members are more-than-likely using the same network. While employees are accessing corporate data, their partners or spouses may be doing the same for other firms and their children may be using remote learning, or just playing computer games. Sometimes, to get outside for a while, employees may work in – or parked next to – local coffee-shops, which offer free, unprotected Wi-Fi.

Given the potential exposures from the WFH environment, companies need to monitor and act to protect corporate security throughout their organization. However, it is important that this should be done in a low-key, non-obtrusive manner. One approach would be for companies to offer full corporate-level security at home, in the office, or anywhere in the world where employees are traveling. This can be seen as a benefit to the employees and their families – while addressing several potential opportunities for security breaches.

Data Leakage from Multiple Sources

Another cause for concern when reviewing corporate data security is the issue of data leakage. Some business-critical data may literally "leak" when applications and data are accessed – on-purpose or by happenstance – by outsiders.

Several sources of data leakage include:

- **Sending email.** A lot of sensitive data exits the enterprise as emails, and more often than not, this is not the result of malicious intent. Employees frequently join a video conference using their personal device and, in the process, they send out an email so that they can quickly log in from their personal device.

- **Sending data to personal devices.** Moreover, employees frequently send business personal information from company devices to their personal ones. Organizations need to allow that to occur while blocking everything else. Conversely, the enterprise has to monitor business activity on personal devices without capturing data that is truly personal.

- **Using business desktops and laptops at home.** In two to three years, the employee's desktop or laptop will end up in a local recycling yard or it will be repurposed outside the enterprise. It may only be an anomaly in a database, but realistically, whether one cares about that desktop or not, the reality is that what happens to the data on that desktop is important. It can become another potential point of data leakage that compromises corporate security.

Passwordless Identification in RBAC World

Passwordless identification is the direction that organizations should be heading toward. We need to get beyond the keying of characters into a slot on a screen. Going passwordless will be a major deterrent to hackers. The objective is to minimize risk from the user, the location, the device and the data.

There are many ways to achieve passwordless identification: Behavior, biometrics, certificates, facial recognition, geographic location, posture checks, IP addresses, QR codes, telemetry, and other non-password prompts can be utilized to determine identification and access rights. And, of course, multi-factor authentication can be added to the combination of security checks.

Furthermore, it should be noted that in this time-sensitive world, continuous authentication is now a requirement, not a nice-to-have. The individual who is using a remote device at any one instant can change to another user. That's why it is imperative that outside users be prevented from gaining access through use of unattended or hacked devices.

Risk Tolerance and Reputational Risk

Risk tolerances will vary depending upon one's applications, and whether it is for business to business (B2B) or business to consumer (B2C). KPIs and KRIs relative to those applications need to take into consideration several forms of risk: operational risk, legal risk, and financial risk.

Converged KPIs and KRIs should include identity data, application performance, monitoring data and vulnerability management data. If these three data sources can be used to tie key performance indicators with key risk indicators, the resulting risk posture will be greatly improved.

SUMMARY

Large companies may have operations around the world, spanning many time zones, but some of the greatest threats to security can occur near to home – wherever that may be – as WFH employees use networking connections and devices that are very different from the ones they used in a highly secure office environment.

CxOs must communicate with the entire IT organization regarding technical adjustments that will improve the company's risk posture across-the-board. Once the security risks have been identified, it is imperative for business executives to communicate with WFH company employees regarding the new directives, the rationale for them, and their responsibility to prevent security breaches by adopting new standard operating procedures for their work-at-home workday.

RFG POV: The WFH hybrid multi-cloud/edge environment creates greater risks for enterprises than was the case in the pre-COVID-19 world. Therefore, Boards of Directors and executives need to be informed of the extent of the new risk exposures created by WFH remote access, along with the methods (and costs) to minimize them. Business and IT executives should re-examine their policies, processes, procedures, privacy, security and governance postures and make the modifications necessary to restore the enterprise to an acceptable level of risk. Additionally, new KPIs and KRIs should be established and reported against – so that executives can become more aware of their organization's current risk status and respond accordingly, if needed.

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 LLC, co-authored this report.

–--