ADVISORY

Today's Top Business Risks and Steps to Mitigate Them

As organizations begin to re-evaluate risks in the context of the "new normal," businesses will need to take steps to identify and minimize risks that may once have been controlled in at least three key areas.

Jul. 06, 2020

When the coronavirus pandemic upended normal business operations, businesses acted quickly to maintain operations and implement safeguards against health risks.

IT departments moved from strategically planning to a mindset of just "get it done." With the velocity and volume of changes, controls and security may not previously have been top of mind.

But as organizations begin to re-evaluate risks in the context of the "new normal," businesses will need to take steps to identify and minimize risks that may once have been controlled in at least three key areas. Here are a few key risks to address with your clients and steps to manage them.

RISK: Expansion into new work environments. In a matter of days or weeks, many organizations had to expand the use of current tools while introducing or implementing new tools to allow users to operate from hundreds or even thousands of new locations. This creates the potential for great exposure, as the ability to store data and information may no longer be restricted or maintained on devices/software under the organization's control.

Mitigate risk by:

1. Training users on the proper use of newly deployed tools.

2. Deploying updated employee security training that highlights special considerations for new work environments.

3. Expanding social engineering testing to increase employee awareness of potential risks of working in a remote environment.

4. Evaluating current versions of software and patch/update accordingly.

5. Scanning the environment for the use of free consumer grade solutions that may not meet the organization's security requirements.

6. Performing user access reviews more frequently to evaluate the appropriateness of administrative rights, which may have been provisioned to meet immediate demands and not subsequently removed.

7. Assessing the user management process, including provisioning and de-provisioning, to validate that new tools are incorporated in existing process and that authentication requirements are being met.

8. Validating that logging and monitoring include any new technology that has been procured.

RISK: Contracts with alternative service providers. As the pandemic gained force, many companies quickly contracted with alternative organizations to address immediate needs or to serve as a backup to existing third party services. A full vetting of the third party terms, availability commitments, financial commitments, and security (including privacy) obligations may not have been possible or reviewed.

Mitigate risk by:

1. Updating the inventory of all solution providers to capture a current state of those providers that were provisioned or de-provisioned in recent months.

2. Reviewing and discussing the results of prior year SOC reports or other control related reporting to baseline the organization's understanding of control ownership, processes, and risk appetite of the contracted service provider.

3. Reviewing and updating budgets to account for new commitments; re-forecast the expected spend on services (such as collaboration services) and the impact on other IT initiatives.

4. Re-assessing the recovery and continuity procedures to validate that new service providers are included and the priority of such services are appropriately classified.

5. Updating risk assessments and business impact analysis to incorporate new technology and reliance on new service providers.

6. For organizations that have data governance programs, engaging with owners to understand where data has transitioned or new services are utilizing data and making adjustments or decisions on how related risks will be addressed.

7. Determining the communication channels you have with your service providers, who is interacting with them, and who has ownership for the relationship. Responsibility of the relationship owner should include monitoring the ability to perform at expected levels and the financial stability of the service provider (i.e. their ability to continue to support the company.)

8. Monitoring the completion of onboarding and training of service providers related to your organizational policies and procedures.

RISK: Supply chain disruptions. Supply chain disruptions have created havoc throughout the economy as demand for some products outpaces supply, shipments

are delayed, and operational issues challenge manufacturers, distributors, and resellers. From an IT perspective, availability is a top concern if a device fails and new products are to be procured or replacement parts are required. Lack of products may have a direct impact on an organization's ability to generate revenue, fulfill obligations to customers, or effectively support an organizations operations.

Mitigate risk by:

1. Revaluating supply chain risks related to new devices, replacement parts, or other IT infrastructure needs or potential needs.

2. Understanding vulnerabilities due to concentrations or dependencies on certain suppliers.

3. Identifying contingency or backup strategies, both how an individual organization will address and the plans of the contracted supplier.

4. Developing strategies to respond to supply chain disruptions. Leverage business impact analysis to determine which services may be ramped down due to a lack of computing power or other IT services.

This list is by no means all-inclusive. But taking action in these key areas should allow your clients to take control of their enterprise and emerge better prepared for the inevitable changes that lie ahead.

=======

Brett Nabors is a partner in Weaver's IT advisory services practice. He focuses on business process improvement, integrated compliance, internal control assessments, IT governance, enterprise risk management implementation and system and organization controls (SOC) reporting.

Advisory • COVID-19 • Small Business • Technology • News