VISIT MAGAZINE WEBSITE

Data Protection in a Changing Work Environment

As companies prepare to bring employees back to the office or transition to a hybrid work environment, it's a good time to review data protection practices.

The timing is right to reevaluate and adapt your data protection practices for a new dynamic workforce as companies bring employees back to the office or transition to a hybrid work environment.

When the COVID-19 lockdowns forced an abrupt restructuring to employees' routines, many organizations scrambled overnight to develop or modify controls to reduce risks. Organizations with strong data management, technology and operational response plans were able to effectively manage business demand and/or supply chain disruptions. They developed stronger security protocols, such as secure remote access, video meeting tools and enhanced data protection protocols, to ensure employees maintained compliance standards when processing sensitive information. Now, some of those temporary fixes may become permanent changes to an organization's operations and its business continuity plan.

"We've seen indicators that some data management security protocols enacted as a result of the pandemic will continue. Within Commercial Banking, our business, technology and operational support centers amplified existing design and security practices to manage data in an efficient, controlled and safe manner," said John Bassett, Executive Director for Data Management, Commercial Banking.

Take time to re-evaluate your data protection practices in the context of your new work environment. Use the questions below to assess what changes might be needed for your data privacy protocols.

continued on next page >

What's in the data, and why?

Know your data. Identify and inventory the categories and sensitivity of data that is processed by your organization. Certain data elements will require special handling and more stringent controls (for example, personal data of individuals and material non-public information). This inventory will assist in assessing requirements of specific laws or regulations about collection, use, transfer, storage, or retention of data and the impact of such requirements on the organization.

Where is the data?

Are your data, applications and services stored onsite or in the cloud? Are there backups in different locations? How readily can those backups be accessed? Do you have an incident response plan for handling scenarios, such as a cybersecurity attack that results in lost or stolen data?

You should also evaluate the security of your data in transit. Even if your server is a fortress, there's a good chance that employees may access Wi-Fi from an unsecured home network. Consider requiring encrypted connections (using a VPN or remote desktop) for all work-related tasks when connecting remotely.

Who has access, and how?

Your employees who are returning to the office may now access and print information that was under a view-only access policy during remote work. Adopt the best practice principle of least privilege, allowing authorized users access to only the specific data they need to complete their duties. Continue to remind your workforce of the need to be diligent when handling confidential data whether in paper/electronic form or being shared verbally.

Require users to create unique, complex passwords (with a combination of letters, numbers and symbols) that are changed regularly. Implement multifactor authentication, which adds additional layers of security by requiring the use of a physical token or a one-time password to authenticate the user.

Are continued investments in technology needed?

Data protection is a continuous process as new technologies, new regulations and global guidelines impact the way organizations store and share personal information. Business leaders should commit to strategic investments in new technologies that strengthen data security, such as remote security enhancements, encryption tools, data loss prevention tools, collaboration tools and metadata management.

Have you designed the right culture?

The biggest risk often isn't technology, but the humans who use it. Business leaders should develop a strong culture of data protection and safeguard practices, and stress the importance of continued cybersecurity education and training. Regular training sessions, such as lunch-and-learns or simulated drills, will help all employees understand their role in protecting data. Leaders should encourage teams to quickly report potential data risk issues and gather regular feedback from employees to help strengthen defense strategies.

Key Takeaways

- Evaluate your organization's data protection standards used during COVID-19 to enhance them for a changing work environment.
- Know your data—where it is stored, how it is used and who has access to it.
- Continuously invest in technology and data loss prevention tools.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Summer 2021.

Explore the full issue

VOLUME 10 | SUMMER 2021

Fraud + Cybersecurity

Stay Vigilant. Stay Protected.

CHASE

J.P.Morgan

J.P. Morgan and Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (JPMC). Any example of cyber or other fraud or loss in this material is for illustrative purposes only; any similarity to any actual event or person is unintended and unfounded. This document was prepared exclusively for the benefit and internal use of the party to whom it is delivered (each, a “Recipient”). The content is not intended as, nor shall be deemed to constitute or contain, advice on which the Recipient may rely; does not constitute in any way JPMC research, and should not be treated as such; and is confidential and proprietary to JPMC. The content may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMC. This is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided is intended to help clients protect themselves from malicious cyber activity. It does not provide a comprehensive list of all types of malicious cyber activities and it does not identify all types of cybersecurity best practices. You, your company or organization are responsible for determining how to best protect against malicious cyber activities and for selecting the cybersecurity best practices that are most appropriate to your needs. JPMC assumes no responsibility or liability whatsoever to any person in respect of such matters, and nothing within this document shall amend or override the terms and conditions in the agreement(s) between JPMC and the Recipient.