EzeCastle
INTEGRATION

The Rush to the Edge

COVID-19 driving rapid change to technology and business operations, creating new risks and compliance issues for Financial Services organizations

TABLE OF CONTENTS

EzeCastle INTEGRATION

The COVID-19 pandemic had a profound impact on global businesses. Many organizations experienced significant revenue loss while having to pivot their entire organization to a pure “Work from Home” (WFH) environment. This was an overnight evolution for many organizations with technology leading the way and enabling the business to work in an effective manner from home. Further, employees across the organization needed to adapt their work habitats, cope with the distractions that came with WFH, and learn new ways to collaborate with colleagues.

Typically, such a fundamental shift or digital transformation comes with significant planning and should be driven by the business, aligning with the overall goals of the organization. However, COVID-19 did not allow for long term planning and strategic projects. Organizations needed to pivot overnight, adding new licensing, products, services, processes, and equipment.

In the IT world, we always say, “with change, comes risk” and with rapid change we are exposed to even greater risks.

With this paper we will highlight salient business risks and potential compliance issues that Financial Services firms need to consider as organizations have evolved into a remote work environment and close the gaps that may exist from “Rushing to the Edge” of the network.

There is no debate, that COVID-19 has fundamentally changed how organizations operate and collaborate going forward. Even as the pandemic eases over time, many organizations will continue to support a remote workforce and even begin to leverage the ability to employ teams around the world. As such, firms need to assess their current environment for risk and compliance issues, develop paths to remediate, and build a strategic roadmap that empowers the remote workforce to collaborate around the world.

The Cloud

Adopting new cloud or SaaS applications during the pandemic, may have been necessary to keep your business moving. However, with the cloud comes a new set of risk and compliance issues that need to be mitigated and managed.

Here are some important things to consider and review:

Authentication:

1. Multi-Factor-Authentication (MFA) is not a silver bullet from a security perspective, however it prevents most of the common attacks and breaches. Every platform, accessible from the Internet must have MFA turned up. Unfortunately, many cloud platforms do not do this by default, and it has to be driven by the organization. Things to check are: SaaS platforms, VPN, Citrix, O365, and G-Suite.

2. Single-Sign-On (SSO) is an excellent way to limit the number of passwords users need to manage, establish one place to go to for all applications, control what devices access your applications, from what geo locations, and administer application permissions. If you are using SSO, make sure you have MFA enabled. Also, check to make sure new or existing apps have been configured properly and that users cannot bypass SSO and access the app directly.

3. Device Trust limits what computers can access cloud applications. Some cloud apps have this functionality embedded as part of the security function or as discussed above this functionality is likely part of your SSO platform. When enabled, this prevents non corporate devices from accessing your applications. This is salient for SaaS apps as firms need to ensure data within these apps can **only** be exported to firm assets. Many people WFH are using personal computers and maybe unintentionally saving things locally or to other personal apps like Google Drive, Dropbox, and One Drive. Ensure controls are implemented to prevent information from being download to a non-firm device (this includes mobile devices and computers).

Information Risk

1. Citrix/Remote Desktops – Are you allowing users to access Citrix or other Remote Desktops from non-corporate devices? If so, make sure you disable file transfer. Also, if you needed to enable printing from home, make sure this is documented in your policies and procedures (WISP) and that you can report on and monitor those employees who have been given exceptions.

2. VPN – Are you allowing VPN from non-corporate devices? I really hope not! If you are, you should shut it down immediately, document reasons why it was done, and review to ensure data was not transferred out of the firm onto a local device.

3. SaaS – As discussed under Device Trust, limiting what devices can access these applications is key to securing your data and avoiding data leakage. Further, SaaS apps should be monitored for changes to the environment, data flowing in/out, who is accessing the application, and where they are accessing it from. Make sure you have geo fencing enable as well. If you do not have employees in a country, then that country should be on your blacklist.

Finally, there are some great products to help manage rich SaaS environments – Cloud Access Brokers (CASB's). They allow for more advanced control and monitoring of your SaaS environment and hook into many of the security monitoring products on the market today.

4. Local Files on Endpoints/Devices should be locked down to prevent users from transferring data off the device when they are not connected to the network. Many firms allow files to be saved locally to a firm computer and sync when you connect to the network. However, if you do not have the correct controls in place an employee can connect directly to the Internet and transfer data. This is also the case for mobile devices, even if you have a Mobile Device Management (MDM) tool in place the configuration and settings need to be applied properly to prevent data from being transferred.

5. Email is another vector for data to be exfiltrated from the firm. When employees are experiencing trouble or lack the necessary tools or access, they often e-mail files to their personal accounts. This is a clear compliance violation and a risk to the firm. Many firms have policies around this, but some likely have not implemented controls to catch the offenders and mitigate this risk. Now is the time to close this gap, update policies, procedures, and controls. If you find scenarios where employees have done this, make sure they are documented and remediated.

Video Conferencing & Collaboration

Launching new instances of Video Conferencing and collaboration tools became common during the early days of the COVID-19 pandemic. Ensuring these platforms have the correct settings now is critical. For example:

- Disable chat or ensure chat logs are being sent to your electronic archive
- Make sure record feature is being managed by compliance or system administrator
- Disable data transfers or allow only for admin if needed
- MFID2 compliance
- Verify that new data sources are searchable in the archive, often new feeds fail or given the volume of request that providers are dealing with it could have been overlooked or still in the queue
- Avoid using free accounts, many of the platforms have consumer versions for free with less security and data controls
- Disable sign-on with social media accounts like Google, Facebook, etc
- Turn on Waiting Room Functionality
- Mute all users, moderator controlled
- Set screen sharing defaults

If compliance has been overlooked or gaps exists, it is best to solve now, document, and maybe even self-report. COVID-19 created an incredibly unique set of circumstances and likely regulators will be accommodating if the issues are identified, the gaps documented, and reported. If a good faith effort is not made to resolve this gaps/issues it could result in fines and additional regulatory scrutiny.

Financial Services is a highly regulated industry and compliance considerations need to be made when implementing new technology. This has historically been a hurdle to innovation within Financial Services and FinTech more broadly. This has a direct correlation to COVID-19 and WFH as many of the tools implemented or expanded on quickly fall under regulatory compliance, i.e. Video Conferencing, Chat, and Document Sharing.

Change Management

Much of the previously mentioned required changes to your existing infrastructure. Hopefully, you were able to follow your normal procedures for Change Management. However, it is best practice to review all changes and ensure proper procedures were followed. Maybe a network admin needed file folder access to research an issue or a user could not open a file and their privileges were changed or elevated. Make sure access control is in order and all changes documented.

The foundation to a good security framework is good housekeeping. Do not deviate from best practices as a result of the volume of work or circumstances. Follow best practices and stay consistent with your server and endpoint patching cycles.

Finally, inventory all apps across the enterprise and ensure that users have not installed any new apps or that they are leveraging other unapproved cloud applications.

Onboarding/Offboarding

Managing employee Onboarding & Offboarding remotely, may have presented challenges to some organizations. A review of everyone joining and leaving the organization over the last several months can act as a good check to make sure accounts have been activated and deactivated properly.

For new employees, make sure the correct permissions were applied to their account and device. Did they need to install software? Were their privileges changed? Are they working from a Home computer?

For leavers, make sure procedures were followed, access terminate across all 3rd party apps and devices. Did you get all devices back? If not, make sure they cannot access firm assets.

Third Party Risk Management

As firms quickly adopted new technologies, they established relationships with new vendors and likely did not follow their typical due diligence process. Now is the time to go back and review these relationships and ensure all the proper documentation is in place.

Also, update your DDQ and reach out to your tier 1 vendors and see if they made substantive changes as a result of the pandemic. If you do not have a formal DDQ, you should think about adopting one now.

Work from Home Analytics

Technology has evolved in such a way to create an effective and efficient remote work environment. As discussed, many firms will continue with some form WFH for the foreseeable future. However, this environment does have some drawbacks.

How do you know everyone is working effectively? How can you measure collaboration in a remote workplace? Are staff working more or less? How does this measure up to the final work product?
All valid questions, and valuable information whether you are in an office or remote. This is not a matter of big brother, but a tool to allow for more productive use of time and firm resources.

Luckily, bringing together data across the enterprise has never been easier and firms can create a reporting framework that answers the above questions and more. Further, you can expose the reports to each employee, eliminating the feeling of “big brother”. If you can see the same data your manager sees, no need for angst.

Look to leverage 3rd party software or technologies partners to help bring together your key sources of data and begin to build reports that help you enable your employees to work more effectively remotely and collaborate on initiatives.

Conclusion

The COVID-19 pandemic has created uncertainty and fluidity in the work environment. As a result, organizations need dynamic IT strategies that align with the business, have a vision towards the future, and focus on security. Technology plans need to be tightly aligned to the business goals and operations, with a transformational theme, rather than the traditional framework of incremental change.

Many organizations are coming to the realization that the lack of vision and investment around IT Strategy has led to challenges and risks in the rush to create a robust WFH environment. Firms are now looking for a pathway to transformational change that includes strategy around security. However, they lack the resources or skillset to build, direct, and execute.

This is where Eze Castle Integration can help. Eze Castle Integration's CIO Advisory Team is led by experienced industry veterans with a track record of driving innovative, with business aligned IT strategies that foster revenue growth and efficient operations. Now is the time to think strategic, reduce risk, and set a clear path for the future. Ask your Eze Castle Integration representative about our Work from Home Transformation and CIO Advisory Services.

About Eze Castle Integration

Eze Castle Integration is a global leader in end-to-end technology solutions to financial and professional services industries. We allow 800 forward-thinking organizations around the world to reach new performance levels through innovative technology solutions that drive business transformation.

Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, India, London, Los Angeles, Minneapolis, New York, Philadelphia, Philippines, Portugal, San Francisco, Singapore and Stamford.

EzeCastle
INTEGRATION