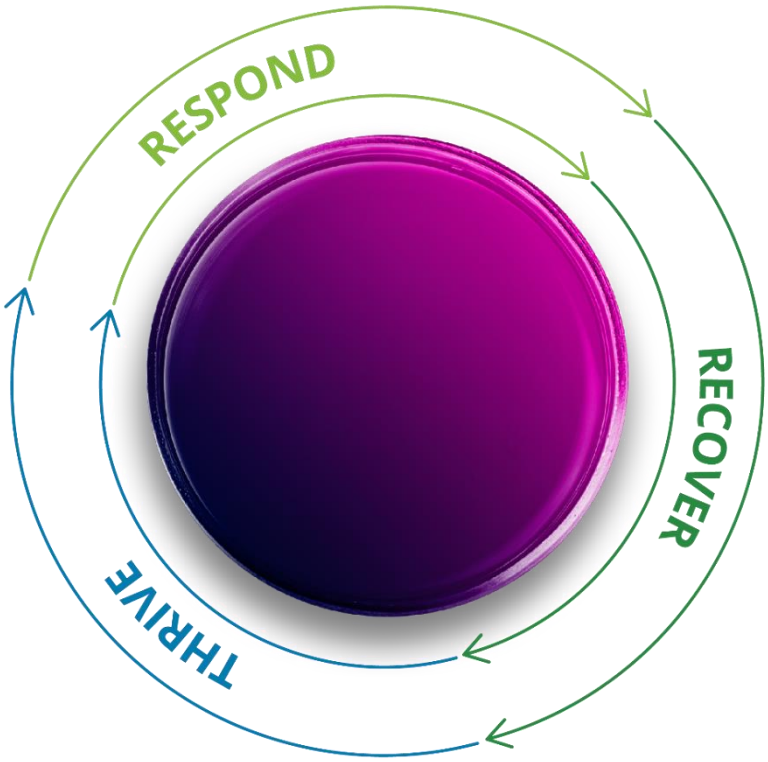
Deloitte.

April 2020



The Q&A roundup series 4: Digital working models amidst crisis–data management, privacy and protection

You asked, we answered.

Here are our responses to the questions you had in store for us, during our webinar on 'Digital working models amidst crisis–data management, privacy and protection'.

Given the current scenario, what steps can an organisation take, from a long-term and short-term perspective, to boost cyber-security and ensure we stay protected?

Currently, we're witnessing a rise in cyber-security attacks pertaining to the global pandemic, and while organisations could evaluate many enhancements, here are a few that should be considered on priority:

- Evaluate the current information technology (IT) infrastructure, to ensure adequate security measures, such as Virtual Private Network (VPN), Data Loss Prevention (DLP) tools, etc. are implemented and functional.
- Install end-point security solutions such as anti-virus and anti-malware programmes, and keep them up-to-date with the latest patches and definitions.
- Perform regular access management reviews to ensure unauthorized users are unable to access content without a 'legitimate and justified need'.
- Disable remote access by default.

- Ensure 'Bring Your Own Device' (BYOD) policies are established, enforced and communicated to users (employees, contractors, third parties, etc.)
- Identify enterprise 'crown jewels' and configure robust security safeguards to protect sensitive data.
- Implement appropriate procedures and tools to promptly identify and report malicious activity. A robust incident response framework could help you analyse and respond in a timely manner.
- Conduct a cyber-security maturity assessment, and based upon its results, formulate a cyber-strategy framework, to align the organisation's cyber risk programme with its strategic objectives and risk appetite.

What is the most common, but ignored, data security best practice that should be followed diligently during these times?

There are many leading practices that should be followed, such as:

- Data classification: Tagging data appropriately, based on its sensitivity, can help eliminate the risk of sharing confidential or sensitive files online.
- Data Leakage Prevention (DLP): Highly targeted risk mitigation configurations, can help avoid data transfer outside an organisation's network.
- Consistent scouting for shadow-IT activities in the network: The IT team needs to vigilantly track and shut down such activities. They should also reinforce the message that users must only install tested, IT approved software, and refrain from installing open-source or free tools without the prior authorisation of the IT team.

How can we raise cyber-security awareness within our 'work from home' employee base, and educate them about best practices?

While there are multiple ways to improve their understanding of cyber-security best practices, here is a handful that can get you started:

- Conduct short and brief e-learning sessions on cyber-security related topics such as, virtual or remote working models, and cover topics like phishing, malware attacks, cyber-hygiene, etc.
- Send awareness e-mailers providing employees with quick pointers for a safe and secure remote working experience.
- Create simulations to help employees identify malicious activities.
- Guide them to refer to trusted government-owned websites and mobile applications for information related to the pandemic and discourage them from clicking on unknown links.

What are the updates your third-party service providers should provide you with?

Organisations need to ensure that third-party service providers or vendors notify them immediately about any data breach or security incident. They should also provide an update about the remediation action taken to resolve the issue. Additionally, organisations should ask for periodic updates on business operations and security measures they have in place, to ensure the safety of your data.

In case organisations need to relax any cyber-controls (such as remote access, etc.) to minimise the impact on its operations and supply chain, then the same needs to be:

- Provisioned after due analysis and authorisation with regards to its potential impact
- Time bound
- Regularly monitored, to safeguard against misuse.

In case there is suspicion of data leakage or theft, what should the organisation do, considering everyone is working remotely? How can we facilitate communication if an employee wants to report a cyber-security breach?

A clear communication matrix needs to be established by the management, and should be communicated appropriately for all employees to refer to, in case of any cyber-security attacks. Organisations can configure a generic email ID and/or an around the clock telephone line to report cyber-security and data breaches.

At an employee level, any suspicion should be immediately reported to their reporting manager, and IT or information security (InfoSec) team, within the organisation.

Secondly, steps should be taken to isolate the computer from the office network and disconnect any active internet connections.

At an organisational level, the following steps may be considered:

- Assess the nature of the incident and the quality or quantity of data leakage.
- Prepare a communication plan for internal and external stakeholders.
- Deploy a "first respondent" team to forensically preserve potential indicators of compromise by using remote data collection techniques.
- Conduct an analysis of the data collected to identify the root cause.
- Seek legal opinion and if needed, report it to the appropriate regulatory authorities.
- Automatic reporting features can be activated through the user's mailbox, to report phishing mails, to effectively prompt reporting of suspicious emails.

How can we ensure privacy readiness for applications that collect and process personal data?

In today's volatile environment, it is important for organisations to ensure protection of users rights and interests throughout the processing lifecycle of their personal data.

For application development, it is advisable to deploy techniques of 'privacy by design' and 'by default' to ensure privacy aspects are taken into consideration from the ground up, during the initial stages of application development.

Organisations should also consider undertaking a privacy impact assessment to proactively identify and address any privacy issues that may arise when applications go-live.

Furthermore, privacy-friendly configurations and techniques such as encryption (to avoid storing data in clear text), anonymisation, and provisions for adequate privacy notice and consent mechanisms can help protect personal data.

What can organisations do in the medium to long term with regards to infrastructure scalability issues?

In the short term, organisations can identify critical applications and databases to boost scale while employees login remotely. They can then migrate their key services to cloud and prioritise access for the appropriate user groups. Organisations must ensure adequate network bandwidth is available and the necessary data governance measures are implemented to safeguard data.

From a medium to long term perspective, they must focus on an infrastructure strategy to migrate services to the cloud and have a multi-pronged cloud integrated approach. They must also focus heavily on process transformation by working with different stakeholders, including the appropriate regulatory and compliance functions. Driving these digital transformational initiatives need to be undertaken on priority so the organisation is ready to take on any future situations that may occur, factoring in all their experiences from the COVID-19 situation. As they review ad-hoc architecture decisions taken during the current period, they can better understand what should be retained or discarded. Organisations may also look at refining the business continuity plans (BCPs) or Disaster Recovery (DRs) plans, based on the perspectives they've uncovered due to the COVID-19 situation.

Does the use of a company's VPN by employees result in a similar secured environment that they would have had in office?

A VPN is used for creating a secure connection to another network over the internet. While it is a vital element to ensure secure connections to the office network, it cannot be relied upon as the sole safeguard. Secure connectivity also depends on other configurations, such as firewall policies, authentication mechanisms, identity and access management, etc. Here are a few mechanisms that organisations must evaluate:

- Review the firewall policies, antivirus configurations, and administrator access policies on user systems, to try to ensure that connections originate only from secure end-point devices.
- Enforce a consistent layer of multi-factor authentication (MFA) or deploy a step-up authentication, depending on the severity of access requests.
- DLP tools could be used to detect and block any data leakage attempt within the network and through user end-points.
- Review and establish corporate firewall rules for remote access, user execution and behaviour analytics (UEBA), file integrity monitoring, to enable appropriate access for remote users.

Do you think that the user's personal computer configuration will matter, if they have been given access to virtual machine (VM)?

We need to consider the end-point (personal computer) configuration and take security into consideration, while providing end users with remote access to VMs. While organisations implement state-of-the-art security on VMs, they must also implement end-point security controls such as, an updated antivirus, the latest security patches, a properly configured firewall, password policy, etc.

Prior to the provisioning of access, an end-user system security 'health check' should be performed, to ascertain compliance to security policies and the access request should be rejected if any deviations are found. The security controls implemented at the end-point should ensure that the user's system does not possess any risk of malware injection, unauthorised access to confidential data, etc.

How can we as an organisation monitor our tax, regulatory and statutory compliance in a remote working scenario?

Assimilation of data is a daunting task for any company, especially in a remote working environment. In these circumstances, it is advisable for organisations to implement an online compliance monitoring framework, including the use of tools with appropriate backups by professional service providers, who have the professional training and resources to track and update all changes in the regulatory and statutory regimes.

Such tools should have capabilities to provide latest advisories, notifications and directives, so that companies can focus on implementation rather than tracking. At Deloitte, we have been helping our clients through the use of our in-house developed tool, called 'Deloitte Compliance Monitor', as well as by sending weekly newsletters to keep them abreast of the changing regulatory scenario.

Are there any tools or solutions offered by Deloitte that provide a summary of tax, regulatory, or fiscal COVID-19 measures, which have been announced by governments?

Most governments across the globe have been responding promptly to the effects of the COVID-19 pandemic, by announcing various tax initiatives and other financial relief to support businesses and individuals. To help keep our clients informed and enable them to navigate through these new tax developments, we offer a couple of complimentary resources:

- We have created a microsite called 'Deloitte Tax Atlas COVID-19 Tax & Fiscal Measures': It provides our clients with a high-level summary of tax and fiscal COVID-19 measures that have been announced by governments worldwide. Clients can filter by country and tax type, in an interactive map and also conduct comparisons by country.
- We have also created 'COVID-19 Signal Alerts': It provides the latest government tax and fiscal responses to COVID-19. Deloitte has collaborated with Signal AI to develop a tax-intelligent news platform that produces daily alerts on COVID-19 initiatives to our clients.

These are some of the ways by which we are helping clients stay updated on tax and fiscal measures introduced by various countries.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2020 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited