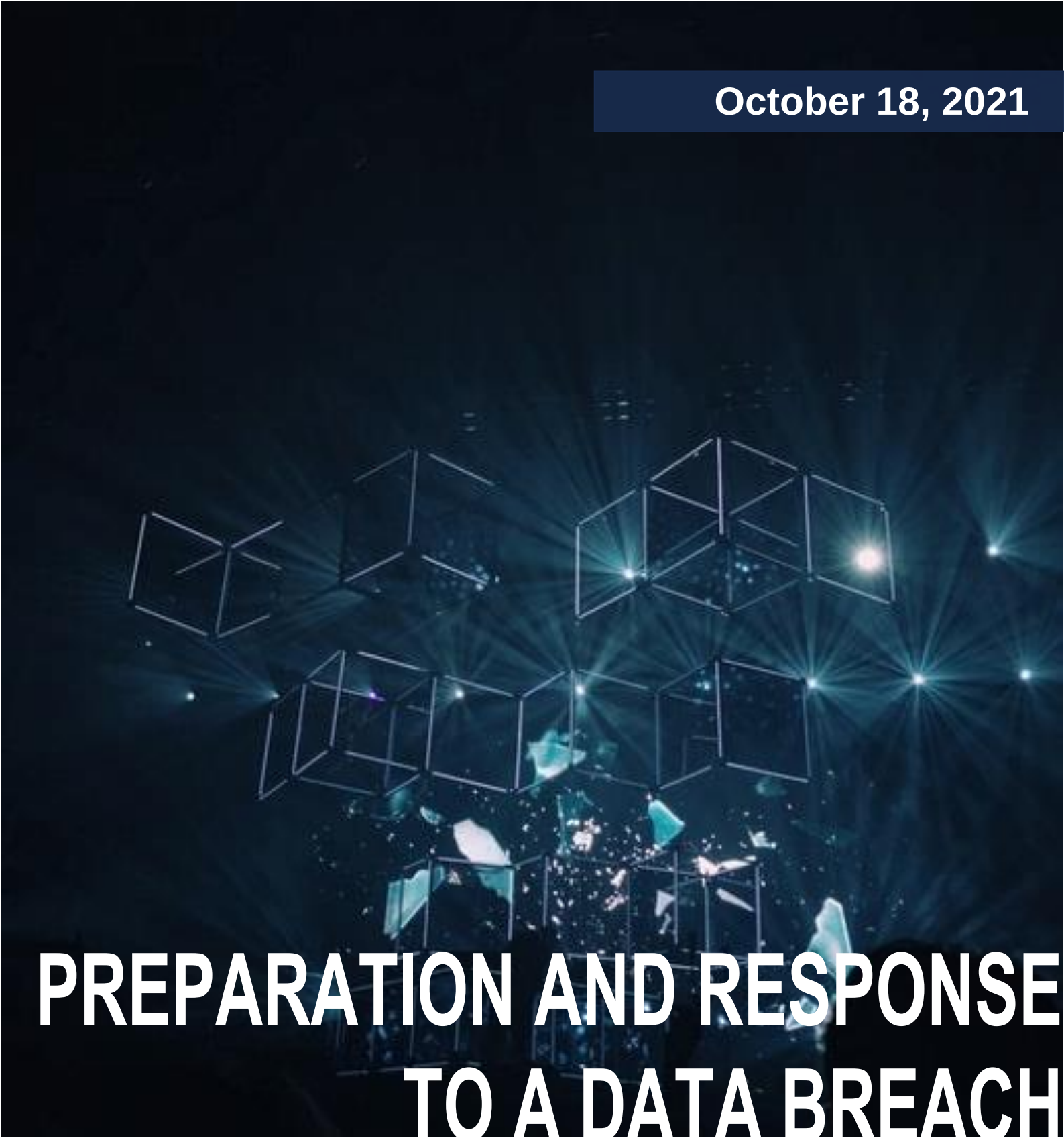
October 18, 2021



PREPARATION AND RESPONSE TO A DATA BREACH

GUIDANCE NOTE

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

Introduction

An increased reliance on technology and the ubiquity of data storage online has led to businesses being increasingly vulnerable to the threat of cyber-attacks. The onset of the pandemic coupled with a shift towards remote work has exacerbated this vulnerability and led to a significant increase in the frequency and severity of data breaches. Businesses frequently find themselves victim to data breaches perpetrated by malicious external actors, employees with insider access, or the inadvertent leaking of confidential data onto the public domain.

A data breach may impose consequential financial costs on a business, with a 2020 report by IBM Security titled 'Cost of a Data Breach Report 2020' finding that the global average cost of a data breach was over $3.86 million. Further, over 70% of business surveyed across the world stated that having a remote workforce increased the risk associated with a data breach, with the report finding the average cost of a data breach to be approximately $4 million when involving a business with a predominantly remote workforce. Stolen or compromised credentials were found to be the most frequent and expensive cause of malicious data breaches, followed by human error and system glitches.

With a large number of businesses finding themselves increasingly underprepared to respond to a data breach, it has become critical for businesses to develop a comprehensive plan that addresses such an eventuality. A regularly updated and enforced data breach response plan is essential to the secure functioning of a business and the protection of its data – the measures set forth below may be employed to mitigate the damage a data breach may cause.

Preparation for a Data Breach

a) Implementation of Security Protocols

Businesses must put in place adequate security protocols to secure data and diminish the likelihood of a potential data breach. Indian legal obligations reaffirm this requirement of having appropriate security standards in place, with Section 43-A of the Information technology Act, 2000 ("**Act**") mandating the implementation of 'reasonable security practices and procedures' and holding businesses liable to person affected by a failure to not implement 'reasonable security practices and procedures'. Rule 8(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**2011 Rules**") states that a body corporate shall be considered to have complied with reasonable security practices and procedures if it has implemented such security practices and standards and has a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. Rule 8(2) of the 2011 Rules recognises the IS/ISO/IEC 27001 standard as one that would be in compliance with the standard required by law. Businesses that are additionally governed by banking regulations and securities exchange regulations may be prescribed different, more specific standards from time to time.

b) Establishing a Response Team

A 'response team' that is empowered to react to a potential data breach incident on short notice is one of the crucial components of having reasonable security practices and procedures in place. The response team may constitute an executive duly empowered to make decisions, information technology personnel to assess the technical extent of the breach, legal counsel and representatives from the company administration to streamline the business's immediate response to a data breach. A combination of internal members and external experts in the response team will facilitate co-ordination between various verticals of the business, while ensuring the requisite expertise to deal with the data breach is at-hand.

To ensure an efficient response, a business should endeavour to set in place systems to immediately notify the response team of any breach in security protocol, as and when the protocol is found to have been violated. Clear guidelines must govern the functioning of the response team, such as specifying the authority to which a breach must first be reported or specifying the core team that is responsible for responding to the breach from the point of notification onwards. Businesses should also ensure that access to documents created from internal investigations carried out in response to the breach are restricted to members of the response team, so as ensure that sensitive information is not openly accessible or further disclosed. Streamlined action by the response team may help mitigate regulatory action in the long run, while also potentially easing backlash from individuals/entities affected by the breach.

c) Controlling the Flow of Confidential/Restricted Information

A business that deals with sensitive information must ensure that the data is not copied or disseminated more than strictly required. This is emphasised by Rule 5(4) the 2011 Rules which restricts a body corporate or any person on its behalf from retaining 'sensitive personal data or information' for longer than is lawfully required, with Rule 5(5) clarifying that information should be utilised only for the purpose it has been collected. In the event of a breach, maintaining strict control over the dissemination of information will enable businesses to be able to efficiently locate the source of the breach and take necessary mitigation measures. The business may also institute systems that provide for communication of sensitive information subsequent to a breach, so as to ensure other sensitive information is not put at risk in case of an ongoing breach.

d) Establishing a Communications Plan

Businesses may create a comprehensive communications framework to streamline communications between the business and individuals/entitles affected by the data breach, which may include customers, employees, business partners, or the public at large. In the event a data breach occurs, the team tasked with communications should be trained to respond at short notice and have suitable capacity to respond to all individuals or other stakeholders that may have had their data compromised as a result of the breach.

Responding to a Data Breach

On notification of a data breach, it is essential that the business respond in a streamlined and efficient manner by taking the following measures:

a) Assessment of the Breach and Data Compromised

On being notified of the breach, the business must immediately assess the extent of the breach and the type/nature of the data compromised. If the breach involves personal data, the business should recognise and classify the various classes of persons who are affected, the number of people affected, and the geographical location they are based in. The business must also assess if the data breach is an ongoing incident and ascertain if the malicious actor continues to have access to the system. It is essential for the business to be able to identify the cause of the data breach and take immediate measures to remove/isolate the cause. Identifying the nature of the actor that caused the data breach, whether cybercriminal, employee, or external service provider, will help identify the root of the data breach. On identifying the cause, the business may take action to mitigate any damage caused by the breach and engage the services of a specialised data forensics team to gain accurate assessment over the extent of the breach.

b) Caution Against Using Compromised Systems

In the event a business finds that its information technology ("**IT**") infrastructure is compromised, the business should restrain its employees and associates from using the businesses' IT

infrastructure for communication (internally or externally), particularly in relation to information regarding the breach, whether confidential or otherwise. A malicious actor that is still within the compromised system may be able to intercept such communications and further exacerbate the damage caused by the data breach. The business may consider utilising alternate modes of communications, such as a secure and uncompromised external email address, to communicate information regarding the data breach response. The business must also isolate affected systems immediately to prevent the further compromise of data. The business may also secure evidence of the breach, including copies of the affected systems, system log files etc. to aid investigation into the data breach – this may also aid compliance with the requirements of the applicable regulatory authorities.

c) Compliance Requirements

On the threat to the IT infrastructure being neutralised, the compromised IT systems being secured, and the extent of the damage being ascertained, the business (with the advice of legal counsel) must ensure compliance with all regulatory requirements. This may include assessing if the data breach may be considered a 'notifiable data breach' under applicable law, and if regulatory authorities, insurers, and/or the affected data subjects are required to be notified. While the Act does not require data subjects to be notified in the event of a breach, the banking regulations and securities exchange regulations may have additional disclosure requirements that have to be complied with. Notification may not always be requisite, especially if there is a high degree of assurance that the data has not been accessed or disclosed- legal counsel engaged may be consulted to ascertain if notification is required in the particular circumstances of the breach.

The Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, specifically under Rule 12 (1), imposes notification requirements on the occurrence of cyber security incidents which include the targeted scanning or probing of critical networks or systems, the compromise of critical information or systems, unauthorized access to IT systems or data, and attacks on servers and databases. Upon the occurrence a data breach, businesses are required to notify Cert-In, India's nodal agency for responding to cyber security incidents, within a 'reasonable period of time'. Businesses must note that other regulatory agencies may prescribe different timelines for reporting a data breach; for example, the Reserve Bank of India requires breaches to be reported witing two to six hours of occurrence.

d) Divulging Confidential Material

On occurrence of a data breach, regulatory authorities such as CERT-In may require the business to produce information/ documentation relating to the data breach. Businesses must also approach the voluntary disclosure of information to regulatory authorities/law enforcement with caution, as the information may find itself on the public domain. Any disclosure that is required to be made must be restricted to the amount necessary.

This paper has been written by Vinod Joseph (Partner) and Pranav Pillai (Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata I Ahmedabad

www.argus-p.com