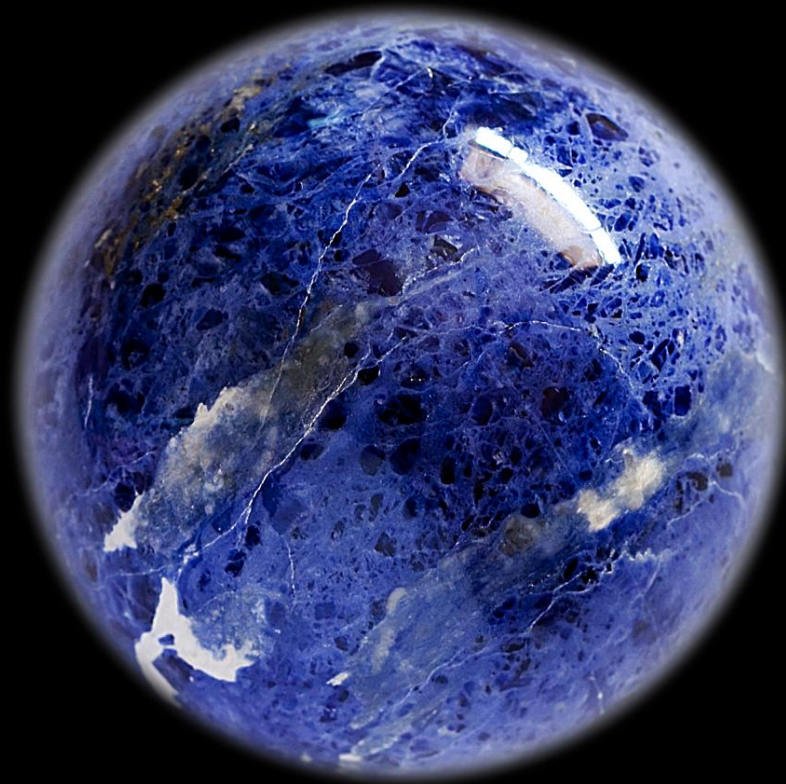


Deloitte.



Role of cybersecurity in M&A

Secure 'now'. Agile 'next'.

2021

The current M&A landscape

- As we enter into the new year, businesses are slowly starting to not just survive, but also thrive in the 'new normal'. While Mergers and Acquisitions (M&A) saw a decline in the past year owing to COVID-19, a revival is expected this year, and cyber risk and cybersecurity will play an imperative role in unlocking key M&A deals.
- Organisations may target others and try to acquire them to add new capabilities to their existing repertoire, to reach new market segments and reduce envisaged competition in the market.
- This process, right from identifying an organisation to acquire to finally acquiring it, involves a thorough inspection before the deal is finalised. Therefore, it is extremely essential to assess the financial, operational, and strength capacity of the organisation during a potential takeover.
- This is where organisations face a challenge. There is a gap in the assessment of information and cybersecurity posture of the involved entities, and the implied risks that it can have for the organisation acquiring it.
- In a recent survey by Forescout*, 62 percent participants agreed that their company faces significant cybersecurity risks by acquiring new companies, and expressed that cyber risk is their biggest concern post-acquisition.



The implications of not conducting a thorough due diligence are serious. In 2017, the price of an American multinational telecommunication's acquisition of a web services provider plunged **\$350 million** as a result of the latter's data breach compromising more than **1 billion** customer accounts.



In a more recent example from April 2020, a pending merger had **5 percent** of its total purchase price set aside to cover the potential fallout from a ransomware attack¹.



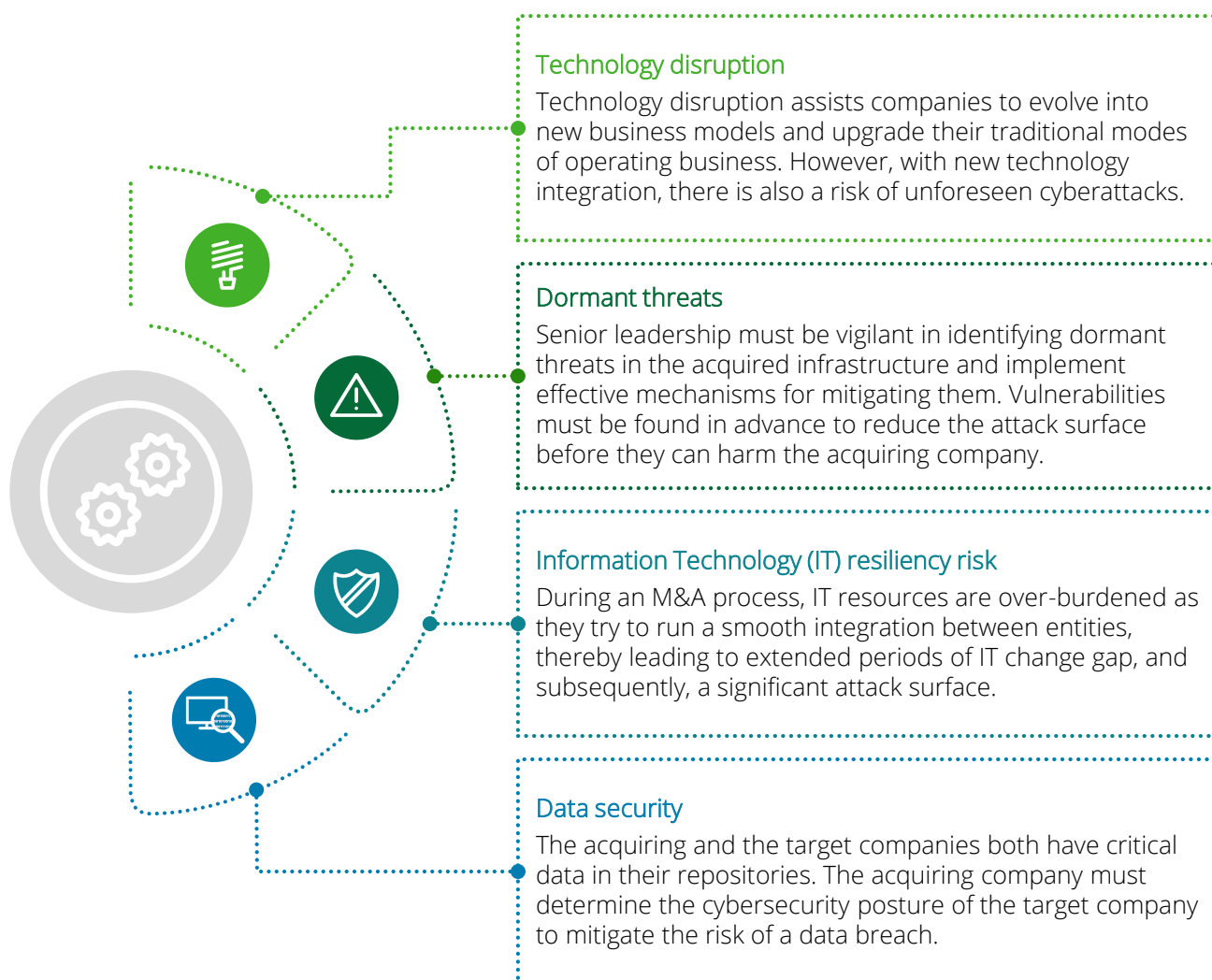
This seems to agree with the data that the Forescout survey report* shared, where **53 percent** respondents stated that their organisations encountered critical cybersecurity issues during the M&A process, which imperiled the deal negotiation.

1. Source: <https://securityintelligence.com/posts/mergers-and-acquisitions-without-cybersecurity-risk/>

* Source: <https://www.forescout.com/company/resources/cybersecurity-in-merger-and-acquisition-report/>

Market need: The importance of cybersecurity in M&A

- Completing an M&A is a high-risk proposition, owing to its potential to influence market dynamics, competition, shareholders interest, business partners, etc.
- Technology also plays an important role by not only enabling the integration, but also driving the new business operating model. It brings in an entire gamut of cyberattacks, and a poor cybersecurity posture can slow down the company's acquisition process and, in some cases, also be a deal breaker.
- It is estimated that by 2022, about 60 percent of the organisations will consider cybersecurity posture in their due diligence process as a critical factor during any M&A².



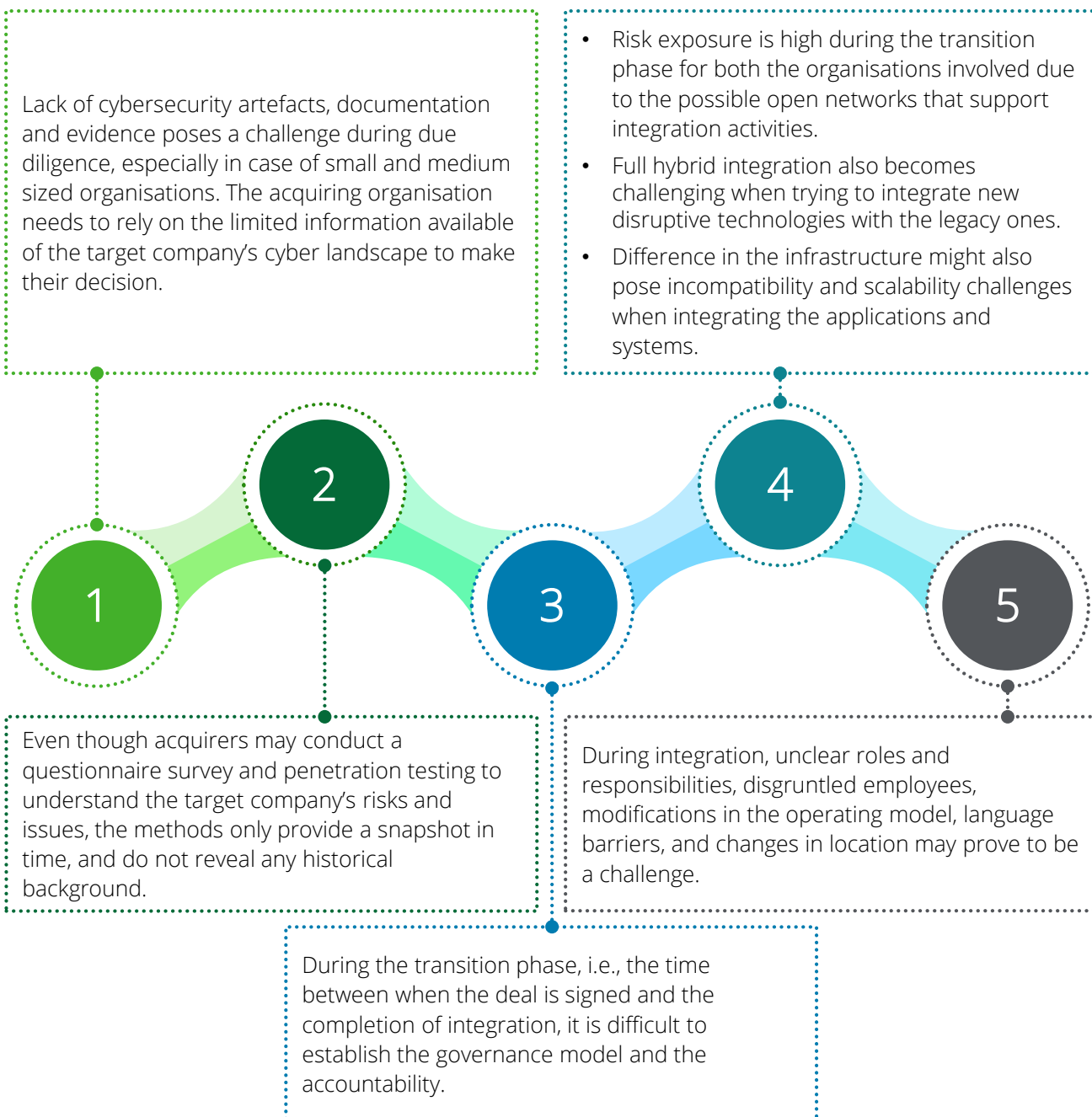
² Source: <https://securityintelligence.com/posts/mergers-and-acquisitions-without-cybersecurity-risk/>



Business challenges during M&A

Business challenges during an M&A

An M&A goes through multiple phases before the final integration is complete. It starts with due diligence and continues through transition right up to integration. Each of these phases poses a different cybersecurity challenge in terms of strategic, technology, and transitional and operational risk. Some of the key challenges during this period include the following:





An in-depth understanding of the M&A lifecycle

We help you manage cybersecurity concerns across the entire lifecycle of the M&A, which includes the process prior to, during, as well as post acquisition. At each stage of the process, we identify the key steps that are imperative for both the target company, as well as the acquiring company to ensure a smooth transition.



Pre – M&A

From initial screening to the start of negotiation

 <p>Key steps required during this stage</p>	Identify the status of the applicable legal and regulatory compliance of the target company, based on the scope of acquisition.	Identify inherent business risks to the acquiring company from the target in the event of an acquisition.	Understand the current InfoSec and privacy risk of the target company by conducting a detailed risk assessment.	Identify early indicators of risk, based on publicly available information and passive threat hunting.
 <p>Importance of these steps</p>	To identify any potential regulatory penalties	To identify if the business risks are within the acceptable limits of the acquiring company	To understand the current controls risk and determine how much effort is required to treat the risk post acquisition	To identify risks before the merger is finalised and uncover the probability of breach occurrence





An in-depth understanding of the M&A lifecycle



During M&A

From pre-announcement to the signing of deal

 <p>Key steps required during this stage</p>	Finalise the type of integration—full, hybrid or soft—to be aligned to the strategy behind the acquisition.	Formulate RACI matrix for InfoSec activities during the merger, based on the type of integration.	Conduct more active threat hunting and penetration tests once the deal is legally signed.	Review InfoSec processes and procedures of the target company to ensure it is aligned with the acquiring company's InfoSec requirements.
 <p>Importance of these steps</p>	To understand the risk for the acquiring company and formulate the risk management strategy accordingly	To establish roles and responsibilities of the target and acquiring company	To proactively identify any critical vulnerabilities and potential security breaches	To streamline and standardise InfoSec processes and procedures for effective risk management





An in-depth understanding of the M&A lifecycle



Post – M&A

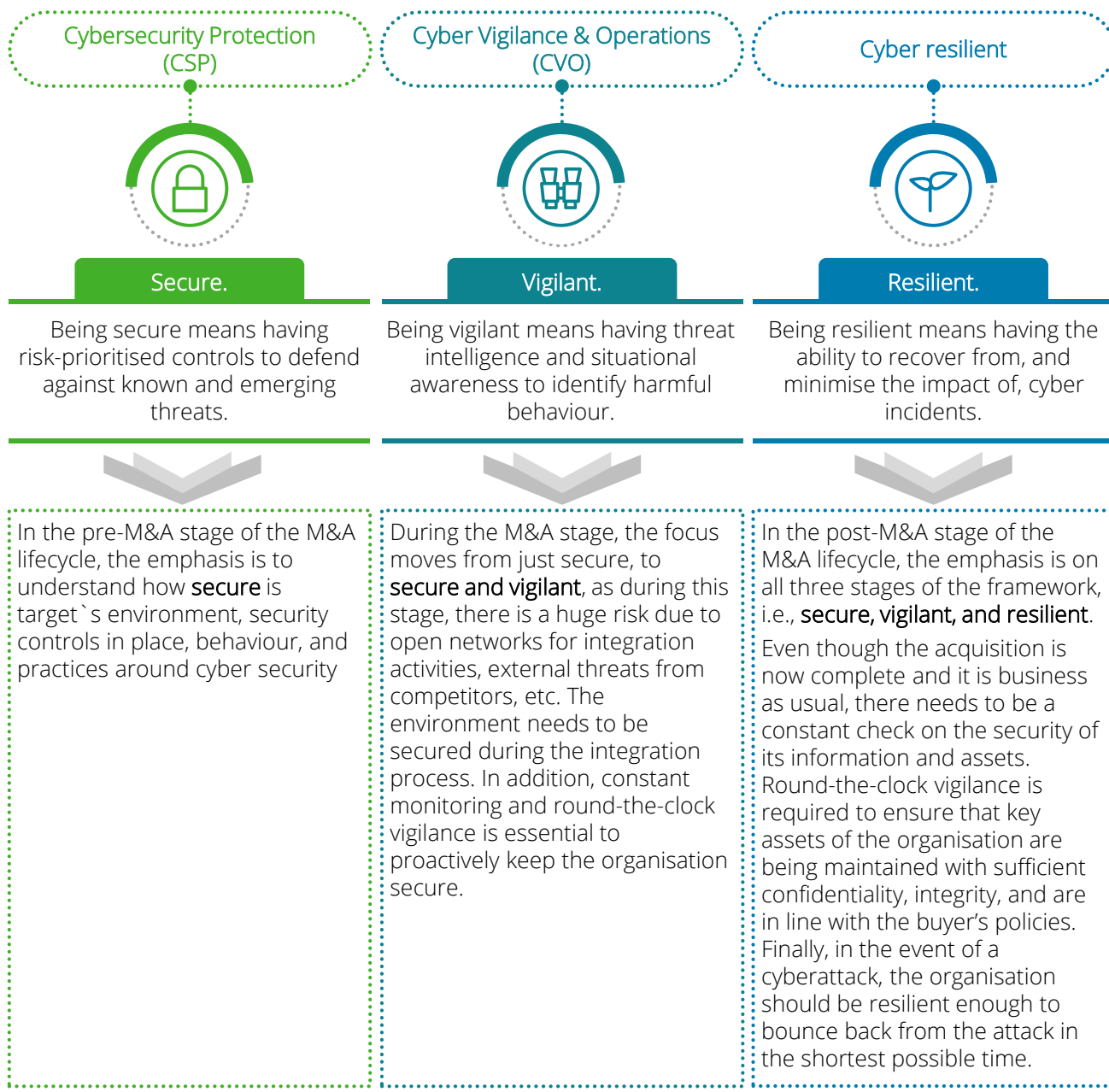
From signing of the deal to integration

 <p>Key steps required during this stage</p>	Establish and monitor Key Risk Indicators (KRI) for ongoing compliance.	Remediate the vulnerabilities identified in the previous steps and establish guidelines for re-assessment.	Establish a governance model for ongoing compliance and incident handling.	In case of full integration, onboard target company's InfoSec resources to acquiring companies' InfoSec services.
 <p>Importance of these steps</p>	To proactively monitor risk levels on an ongoing basis and ensure that risk is kept within acceptable limits	To treat risks identified during the merger and perform re-assessment periodically	To ensure incidents are identified and handled effectively	To extend existing InfoSec services to the extended organisation



Our Secure. Vigilant. Resilient. framework

Our **Secure. Vigilant. Resilient.** model provides a comprehensive set of service offerings to support your organisation's M&A process throughout its complete lifecycle. Our framework helps you develop a cybersecurity programme in line with your organisations' strategic objectives and risk appetite.



Through our key capabilities of **analytics/risk intelligence, training and integrated solutions**, we can support the delivery of your M&A services.

Our Secure. Vigilant. Resilient. framework (contd.)

While delivering our services defined under **Secure. Vigilant. Resilient.** framework, following are the essential components to be considered for an effective and efficient cyber risk management in the M&A lifecycle.



Our Secure. Vigilant. Resilient. framework (contd.)

Key cyber risk focus areas for M&A

To achieve and maintain a **Secure. Vigilant. Resilient.** posture, it requires an ongoing effort to define an executive-led cyber risk programme, track progress, and continuously adapt the programme to shifting business strategies and the evolution of cyber threats. The key cyber focus areas during an M&A are:



- Cyber/IT due diligence
- Cyber risk assessment
- Privacy due diligence
- Vulnerability assessment and penetration testing
- Cyber Maturity Assessment
- Breach assessment



- CISO as a service – Transition service
- Cyber strategy alignment
- Application security
- Cyber transformation during M&A
- Privacy compliance and readiness
- Cyber threat monitoring
- Identity and access management
- Secure data migration strategy
- Third-party risk management



- Cyber awareness
- Cyber post integration assessments and compliance (application, IDM, technology)
- Post application reviews
- Cyber incident response
- Regulatory compliance
- Data governance and privacy
- Privacy reviews

Managed services







Our tailored, high-touch managed and subscription services can help clients operate more efficiently, address talent shortages, achieve more advanced capabilities, and keep on track with client's overall cyber risk programme objectives.



The Deloitte difference: Key benefits

The Deloitte difference: Key benefits

Our holistic approach, combined with years of industry experience, sets us apart from the crowd.

-  Our mature practice on M&A ensures that we have a treasure trove of knowledge on the subject.
-  Our experience in Cyber Risk Advisory, along with our expertise in the M&A sphere, enables us to assist you in ensuring seamless integration with your acquired businesses.
-  With our business-focused information security risk assessment methodology, we provide you with a realistic view of the risk exposure against your acquiring businesses.
-  Our professionals are uniquely placed to understand the cyber risk landscape of your organisation from a business need perspective, and can identify and analyse key risks and challenges in an M&A scenario
-  Our technological capabilities help you understand the risk at an early stage of acquisition, which in turn enables you in effective decision making.
-  Our experience in M&A space with clients from both sides (acquiring and acquired companies) has helped us gain a holistic understanding and insights into the potential key risk areas during any M&A.

Conclusion

Managing cybersecurity during M&A cannot be a one-time activity, but needs to be an ongoing process throughout the entire acquisition lifecycle. The more due diligence a company performs with respect to cybersecurity during a M&A, the better their outcomes are when it comes to reducing risk, protecting the company's assets and ensuring a smooth transition.



Connect with us



Rohit Mahajan

President - Risk Advisory

Deloitte India

rmahajan@deloitte.com



Gaurav Shukla

Partner, Risk Advisory

shuklagaurav@deloitte.com



Deepa Seshadri

Partner, Risk Advisory

deseshadri@deloitte.com



Key Contributors

Runa Dalal

Sowmya Vedarth

Vageesh Srivastava

Deloitte.

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 has been prepared by Deloitte Touche Tohmatsu India LLP (DTTI LLP), a member of Deloitte Touche Tohmatsu Limited, on a specific request from you and contains proprietary and confidential information. This material may contain information sourced from publicly available information or other third-party sources. DTTI LLP 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. The information contained in this material is intended solely for you. Any disclosure, copying or further distribution of this material or its contents is strictly prohibited.

Nothing in this material creates any contractual relationship between DTTI LLP and you. Any mutually binding legal obligations or rights may only be created between you and DTTI LLP upon execution of a legally binding contract. By using this material and any information contained in it, the user accepts this entire notice and terms of use.

©2021 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited