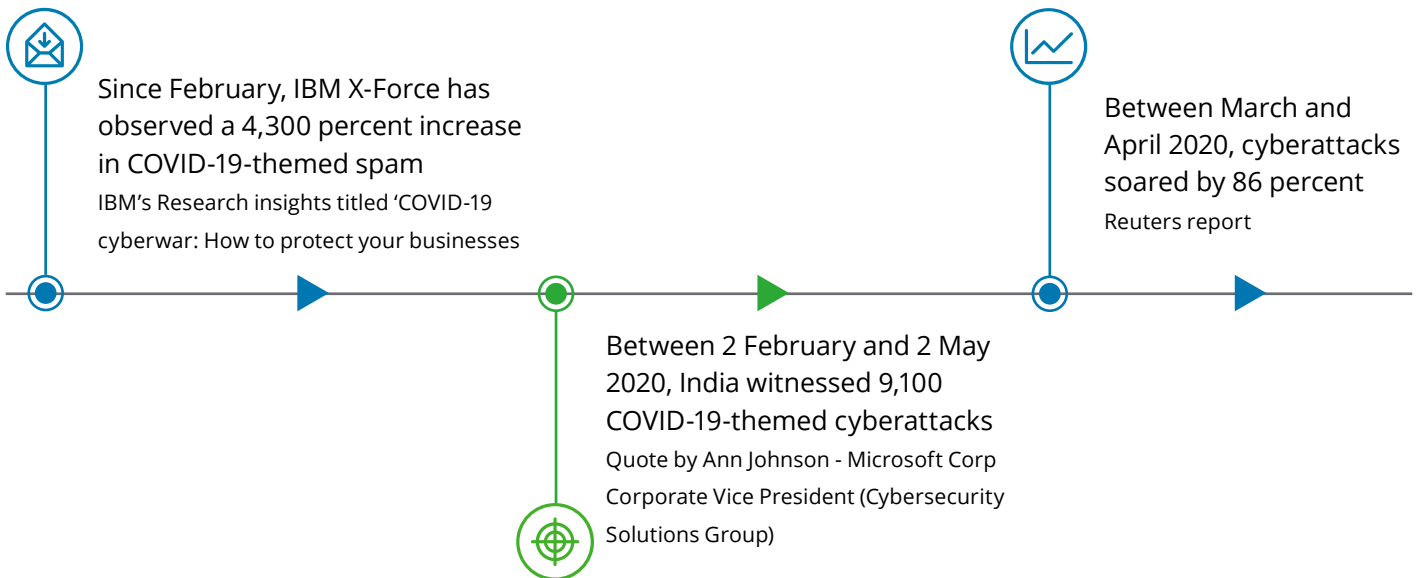









Unlocking the value of Cyber Insurance

August 2020

The ongoing pandemic has affected all the aspects of our lives, from the way we live to the way we work. COVID-19 has had a significant impact on the cybersecurity space as well, as is illustrated through the statistics below:



The sudden increase in cybersecurity threat vectors can be attributed to the following reasons:

-  **Increased security risk from remote working**
The COVID-19 crisis has forced organisations to switch to remote working without adequate planning and security considerations. This is making them more vulnerable to cyberattacks than before.
-  **Failure/potential delays in detecting and responding to cyberattacks**
Currently, organisations are working with limited staff and have remote access to systems, which has led to delays, and in some cases, failure to detect potential attacks and take corrective actions.
-  **Exposed physical security**
Physical security of information assets has also been exposed due to insecure teleworking practices and distributed residence of data in uncontrolled environments.
-  **Influx of cyber criminals**
The ease of cyberattacks, coupled with the panic caused by the pandemic, has enticed more cyber criminals to attempt cyberattacks.
-  **Failure of Business Continuity Plans (BCP) to feature pandemics**
The unexpectedness of the pandemic revealed that most organisations had disregarded pandemic-related safeguards in their BCP. This led to a lack of preparedness for addressing the COVID-19 pandemic

How can organisations increase vigilance and resilience to combat cybersecurity threats?

Organisations can combat the elevated risks of cyberattacks and data breaches if they:

- Create cybersecurity awareness amongst their employees,
- Monitor and manage availability of business applications,
- Enhance security monitoring of business applications and systems, and
- Revisit BCPs.

Cyber Insurance: Imperative for a secure future

Although the above practices can make organisations vigilant and resilient to cyberattacks and data breaches, the sheer urgency to protect the organisation makes cyber insurance the need of the hour and a critical risk management tool.

According to IBM's Cost of a Data Breach Report-2019,



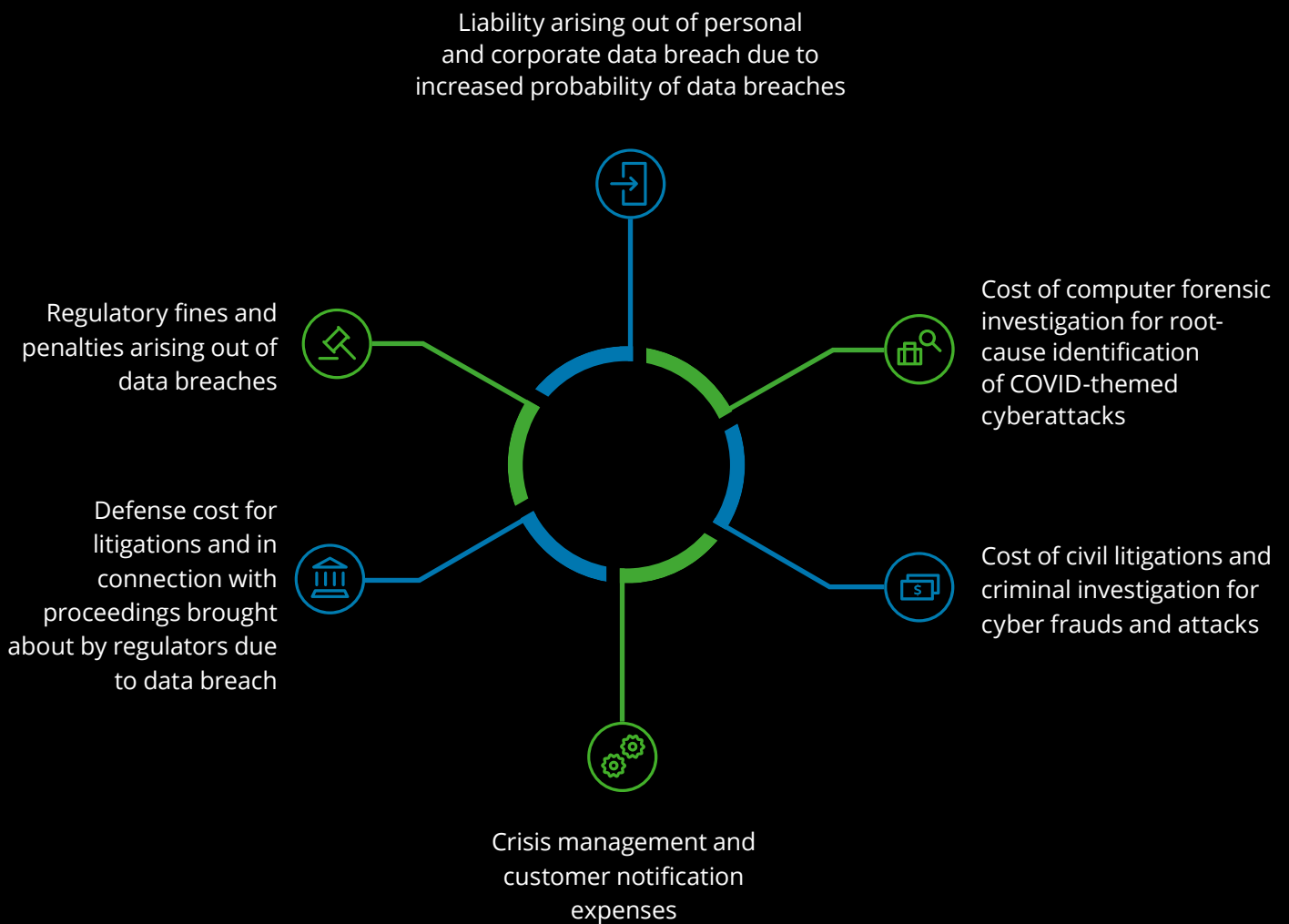
The high financial impact, increased probability of risk materialisation, and existing disruptions in business test an organisation's risk appetite. Cyber insurance helps to cover and mitigate the financial risk of a cyberattack and data breach.

Cyber insurance, unlike general insurance, cannot be picked off-the-shelf. Organisations must carry out an in-depth risk exposure evaluation and identify a tailor-made insurance policy per their organisation's requirements. It is pivotal that organisations select a cyber insurance policy that resonates with their threat exposure.

As the pandemic continues, risk professionals need to work with their insurance advisors to carefully review their requirements and select an insurance policy best suited for their organisations.

Selecting the right cyber insurance policy

It should ideally provide coverage against network security liability, privacy liability, security response and forensic costs, data recovery and restoration, ransom event costs, reputational harm, network business interruption and associated expense, system failure, contingent business interruption, and privacy regulatory defense. In addition, organisations may also consider the following aspects:



It is imperative that an organisation reviews its cyber risk management programme and actively considers an appropriate cyber insurance policy to address the elevated risks owing to the pandemic.

To gain an in-depth understanding on cyber insurance, [click here](#) to read our detailed report on Unlocking the Value of Cyber Insurance.

Contact details

Anthony Crasto

President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar

Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla

Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura

Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Deepa Seshadri

Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Anand Venkatraman

Partner, Risk Advisory
Deloitte India
anandv@deloitte.com

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 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.