Crowe

Cybersecurity Risks for Professionals

Crowe Advisory Services (India) LLP

Audit / Tax / Advisory

Smart decisions. Lasting value.

Introduction

Digitalisation has become an essential part of business in recent years; COVID-19 pandemic has simply forced the hand of the unwilling; and even of the untutored. Increased use of technology has become an essential part of life for professionals and their families.

Efficiency has meant receiving and reviewing documents on smart phones and tablets. As professionals work long hours and against harsh deadlines, we work with soft copy data transmitted and accessed over email and other systems; we save core data, and then drafts and versions on computers and servers. From these same systems we access data rooms and data servers of clients – for audits and assurance work, due diligence, and other professional matters.

During the recent lockdown (and continued WFH) how invaluable has it been to have data on the cloud and remote access capability. How could we have completed audits and other engagements, or to appear in legal processes and judicial matters, without remote access to client data or without downloading data to personal devices. Without technology, how would we have participated in group discussions, presented webinars, held Board meetings, held review meetings.

This has already exposed all of us to risk of data breach. Continued WFH (full or partial) will only aggravate the risk.

Make no mistake – without adequate digital security, the cyber risk exists in full measure even when working from office because data download, storage and transmission will continue to happen through the digital medium.

Are Law Firms subject to digital risk?

The answer lies in just a few quick questions.

- Do you (and now will you) receive, send and store data digitally?
- Do you handle data that may be of interest to others? M&A deal matters, copyright matters, taxation issues, commercial negotiation details, divorce matters, family settlements and many others?
- Could your client's litigation, commercial interest or competitive position be impacted if a data leak relating to the matter were to occur from your office?
- Would you be in breach of client confidentiality commitments or of professional ethics breach if material from your office were hacked and leaked?
- Would you like to not be the cause of entry point into a client entity's data environment?

Professional Firms are digitally active and data heavy; they are attractive cyber targets

Risks for Accountants and Consultants too

Besides matters applicable to Law Firms, additional risks may arise from the following situations:

- Handling audit data and financial results of listed companies
- Handling audit, tax, accounting and payroll data of companies, partnerships and businesses – data that the clients would like to keep confidential
- Confidential assignments concerning M&A, strategies, valuations and impairments – information that the market and competitors would be keen to have access to.

Law firms, audit and tax firms and consultants are lucrative targets for hackers, due to the very nature of their business. Be it financial data, strategy, M&A, direct and indirect taxation, legal and regulatory compliances, personal matters or litigation, these professional practices handle large volume of sensitive, confidential and critical business data. Litigation and arbitration is increasingly being carried out online. Losing or exposing such data could attract financial, legal or reputational risk as well as personal distress to the client.

The common error

Lack of awareness followed by lack of acknowledgement are fundamental problems – it is important to be aware that digital risk can occur in myriad ways. It is then important to get over the "wont happen to me" false confidence – do not make the mistake of assuming that you are not attractive to a hacker.

The next set of errors are around the assumptions that some routine and basic protective measures safeguard you fully – passwords, firewalls, anti-malware protection; these are better that having nothing but are not, by themselves, adequately protective. The rules, policies and practices underlying these can be dilutive of the beneficial value; the method of use and transmission of data can open up your entire systems to a hackers benefit.

The third is to be confident that the system check done once is a long-term guarantee. It is not – just as health checks are not, and must be repeated every year, and even more frequently for the more vulnerable.

Awareness, acceptance, solidity and constancy must underlie your approach to digital risk protection

Recognise that even the most sophisticated systems are vulnerable. The route in could be something out of the ordinary, like what happened with Target whose systems were hacked through vulnerability of their utilities management vendor.

Digital Transformation

Those who already started the digital transformation journey early are reaping the benefits of their investments and will continue to need upkeep. Those who stayed at shore must realise that they need to catch-up fast in the unforgiving pace of the world.

The Challenge

Digital transformation is incomplete without dealing with associated cybersecurity risks. Adopting technology in your operations does not, by itself, cause cybersecurity risks to be resolved – in fact, the technology adoption creates and adds to the risk. Digital transformation encompasses cyber security risks and resolution; but resolution of cyber security risks does not happen of its own. Cybersecurity measures need to be consciously added for a holistic transformation.

As professional practices pursue the path of digital transformation, the associated cyber security risks must be addressed as well – these measures often take a back seat due to:

- Lack of awareness on the part of key decision-makers;
- Skewed project timelines;
- False sense of security through perfunctory action
- Limited budget allocation, with concentration on IT products, software and services

If cybersecurity is not part of leadership discussions, any digital transformation program might exponentially increase the business risk.

Why cybersecurity is relevant to everyone?

Based on 2019 and 2020 Global Risks Report of World Economic Forum, cyber security risks are among the top 10 global risks in terms of likelihood and impact.

Wealth is always subject to the risk of crime. Data, being the new gold, is materially subject to theft, misuse and ransom – and needs to be protected from these risks.

A common misconception is that the small and the unknown are not targeted. But in reality, not all cyber attacks are with initially targeted intent - many attacks are like commercial fishing. Once you are caught on the net, the criminal advances to the next phase of data exfiltration, ransom or disruption.

Addressing the Risk

Cybersecurity must be addressed strategically considering long term business interests. Staggered and incident based mitigation and investment turns out to be ineffective and costly in the long run.

Towards this end, cybersecurity must be treated as a business challenge and must become part of board room / leadership discussions and strategy.

Approach

Different organisations have different business needs and are at various stage of maturity in terms of cybersecurity.

Given the importance of confidentiality and integrity for law firms, accountants and consultants, it is important to analyse how client data and documents are received, transmitted, shared, stored, accessed, archived and

disposed. Right of access, control over changes and transmission of information are critical and need proper audit trails. Establishing chain of custody of important legal, financial or corporate documents is very critical.

Key steps for a cyber-risk management programme would comprise

- Gap and vulnerability assessment
- Risk analysis relevant in the operating context of the professional practice
- Curative and preventive measures
- Cybersecurity risk management framework and policies
- Training
- And above all, creating the right culture towards cyber risk

The process may negate a lot of beliefs and sense of false security; at the end it should also give comfort. Most importantly, it should create the discipline to have and implement a vigorous policy and process.

Conclusion

COVID-19 has presented an unprecedented situation and will change the way professional services are delivered. Technology, an element of WFH and remote access are inevitable as a continuing feature.

In this scenario, it is imperative to consider cyber risk and data protection as a core component of the conduct of professional practices and delivery of professional services. Professionals will do well to assess the cyber risk associated with the new approach and consider applicable controls to bring down the cybersecurity risk to acceptable levels.

About Crowe India:

Crowe Advisory Services (India) LLP provides Risk Advisory, Corporate Finance, Taxation, Business Advisory, Digital Security Consulting, Data Sciences and Business Process Outsourcing services.

We have offices in eight cities in India.

We are a member of Crowe Global, the eighth largest accounting and consulting network worldwide, with 765 offices across 146 countries.

Key Digital Security Contacts:

Anil Aravind, Director, Digital Security Services
anil.aravind@crowe.in

Abhijeet Nath, Director, Digital Security Services
abhijeet.nath@crowe.in

Sreejith UG, Cyber Security Lead
sreejith.ug@crowe.in

1105 Embassy Centre,
Nariman Point,
Mumbai 400021

+91 22 6631 1480
www.crowe.in

Disclaimer: