MARCH 2022

CYBERSECURITY: WHY THIRD-PARTY ATTESTATION IS CRITICAL TODAY

AS CYBERSECURITY THREATS INCREASE IN NUMBER AND COMPLEXITY, IS YOUR ORGANISATION DOING EVERYTHING IT CAN TO PROTECT ITSELF?

Cyber Risk is at the Top of the Corporate Agenda in 2022

Cybersecurity threats are increasing around the globe, growing more complex and affecting organisations of all sizes and industries. Cybersecurity issues can result in financial losses, operational disruption, legal consequences, and reputational damage. Yet many organisations around the world report that they remain unprepared for this critical area of risk.

Twenty percent of global C-suite executives we surveyed in our 2021 Global Risk Landscape listed cybercrimes as the area of risk that they are least prepared for. According to BDO's 2021 Middle Market Digital Transformation Survey, the numbers are even more concerning for middle market businesses:

Nearly **50%** of middle market executives believe that cybersecurity and data privacy risks are their top IT resilience challenge

34% say cyberattacks or privacy breaches are their top digital threats.

Major recent cyberattacks at vendors, significantly impacting their customers, include:

- **SolarWinds Malware Attack:** Attackers inserted malware into SolarWinds' Orion software. Malware was pushed to ~18,000 customers, and attackers were able to remain in the affected organisations' environments for months undetected.
- **Hafnium Microsoft Exchange Hack:** Hacking group Hafnium exploited vulnerabilities in Microsoft Exchange, giving them access to the email accounts of at least 30,000 organisations in the U.S. and 250,000 globally.
- **Kaseya Hack:** In July 2021, hackers compromised over 1,000 companies by targeting software vendor Kaseya, affecting governments and businesses around the world. Kaseya was forced to shut down its servers and recommended all customers to cripple their on-premise VSA servers.
- **Zero-day attack on Accellion:** Accellion, a secure file-sharing and business collaboration company, fell victim to a zero-day attack that targeted its file transfer application software. Hackers used the company's data to launch a broader cyberattack on Accellion's partners and customers.

How Prepared is Your Organisation - and Your Vendors - for Cyber Issues?

Cybersecurity risk is a critical focus area for C-suite executives and board members globally. But it is crucial to remember that this risk needs to be managed not only for a company's *owned* IT infrastructure, but also when IT infrastructure and services are *outsourced* - which is more and more common today.

Outsourcing IT functions - or any critical business function for that matter - brings an additional layer of risks. Even when IT or other services are outsourced, it is still your organisation's business data and your reputation on the line if a vendor experiences a data breach or fails to provide the expected service.

> "YOU CAN OUTSOURCE YOUR ORGANISATION'S PROCESSES AND INFRASTRUCTURE. BUT YOU CAN'T OUTSOURCE RISK.

The Value of Third Party Attestation for Cybersecurity

Third party attestation (TPA) involves certifying the processes of outsourced service providers to ensure the proper procedures are being followed. As organisations deal with a rapidly evolving set of risks and challenges - and increasingly outsource non-core activities - TPA has become an increasingly important tool for creating trust within organisations and across external vendor and client relationships.

For example, many organisations outsource cybersecurity efforts to a dedicated provider with cybersecurity expertise. This is understandable - for many companies, cybersecurity is not a core competency. But outsourcing these procedures brings along its own risks, including potential reputational, compliance, privacy, financial, and operational risks if an attack were to take place.

TPA offers an objective lens to certify that processes consist of best practices and follow adequate controls. For example, an organisation could use TPA to certify that it has the required operations, controls, and technology in place to proactively combat cyberattacks and safeguard against data breaches. While there is no guarantee that the organisation will be protected from a breach or other security incident, the company's clients and vendors have assurance that the company is doing what it can to protect itself.

How BDO Can Help

BDO's experienced advisors take a measured approach to working with clients depending on their unique needs and circumstances. Our TPA approach to cybersecurity includes the following steps:

- Assess the organisation's current cyber program
- Conduct a readiness assessment and gap analysis and recommend remediation strategies
- "Certify" the organisation's information security processes and controls in place

For more information on the benefits of TPA for cybersecurity and other key organisational issues, see our recent paper, Third Party Attestation—a Strategic and Systematic Approach to Managing Risks. For a tailored approach on how you can improve your organisation's approach to cybersecurity, please contact Jeff Ward or Christophe Deams.

Martin Hořický
Partner; IT Consulting
+420 608 937 408
martin.horicky@bdo.cz

Tomáš Kubiček
Partner; IT Consulting
+420 737 210 682
tomas.kubicek@bdo.cz

BDO