Published on *The National Law Review* https://natlawreview.com

COVID-19: Triggering Event for Reassessing Risk and Adequacy of Data Privacy and Security Controls

Article By:

Peter J. Guffin

COVID-19 measures have driven workplace operations beyond what most businesses ever planned. The constructs of a remote workforce and virtual interactions between teams and customers are going to be major components for how business is conducted for the foreseeable future. Many businesses are even seeing potential benefits from these scenarios, like savings in physical office needs and reduced lost productivity from travel—and looking to make these permanent.

With most people working from home networks and using a combination of company and personal devices, the ecosystem of data and processing has significantly expanded and changed. The effectiveness of tools and methods to monitor and identify threats is different within this new operating model. As a result, organizations must reevaluate their cybersecurity and privacy risks and controls and make adjustments as necessary to ensure that they are adequate to protect their data and systems for the “new normal” that is here to stay.

Are your current control measures still adequate to protect your data and systems in this new COVID-19 era?

Compliance and Threat Drivers

For organizations in highly-regulated industries such as financial services, health care, transportation, and food supply, existing regulatory requirements mandate that they reassess their risk profile whenever there is a material change in their operating environment, and verify the adequacy of the measures to handle those risks.

In addition to regulatory requirements, significant increases in external criminal activity—as well as internal originating threats—are affecting business of all sizes and across industries. The expanded use of technology, and the myriad ways in which people are connecting and interacting, has provided new opportunities for those looking to exploit vulnerabilities and cause harm. Cases of fraud, data breaches, and ransomware, to name but a few examples, have increased at an alarming rate since the start of the COVID-19.

The World Health Organization (WHO) has reported a fivefold increase in cyberattacks since the COVID-19 pandemic began. INTERPOL has issued warnings over COVID-19-centric attack

methods targeted at businesses. US-CERT has issued Alert AA20-099A on COVID-19 related exploits.

Covering All Bases – Internal, Third Parties, and Customers

Companies must take a comprehensive look at the new state of their data and processing ecosystems to understand their current risk posture. This includes review of your internal systems and processes, as well as obtaining insight into measures taken by third-party organizations with which your company interacts, including service providers, business partners, and customers. Virtually all entities, large and small, have been affected by COVID-19 measures in at least some way.

Companies need to look at access controls, interfaces, software/firmware update management, monitoring, and threat identification across all their systems and devices. Policies and procedures should be reviewed for applicability and scope. Training and support measures should be validated against the current operating environment. Use of tools, services, and processing provided by third parties across all parts of the company should also be examined.

Every entity that handles your data is another link in the chain of possible exposure. These third parties are dealing with the same evolving set of challenges as your organization. Thus, coordination and validation of how those third parties are protecting your data must be an ongoing process and not a one-time checkpoint.

Another area to pay particular attention is how your team connects and interacts with customers—and how those customers are interacting with your team. New and varied communication platforms and the ability to exchange different types of data open up a number of possible vulnerabilities to consider while balancing the needs of maintaining relationships and providing a positive customer experience, along with data and access protection.

Assessing Risk Holistically: Legal, Technical, and Relationship Factors

When companies look at cybersecurity and privacy risks, there is often a natural inclination to look at technical and legal risks independently based on different ownership and supporting teams. This separation can overlook important gaps and pitfalls.

To ensure completeness, companies should take an integrated approach to risk assessment because technological and legal considerations are inextricably linked in today's operating environment. This vantage point must look internally as well as externally to all parties that have any interaction with the company's people, data, and systems, no matter how transitory or minimal it is.

Getting Started

Effective risk assessment requires having a good handle on what your current data and systems ecosystem look like, being able to account for all major processing operations, and knowing where all of your data is at all times. This can be quite a complex undertaking in some operating environments, but it is critical to having a solid foundation to understand your true levels of exposure and how you can proactively address them. With this information, companies can best identify the full range of threats they face and assess the capabilities they have in place to mitigate those threats.

This post was co-authored by Christopher J. Bender, Northcross Group. Mr. Bender will be joining me on a panel at the Practising Law Institute's December 2020 virtual seminar, "Fundamentals of Privacy Law 2020."

©2024 Pierce Atwood LLP. All rights reserved.

National Law Review, Volumess X, Number 302

Source URL:https://natlawreview.com/article/covid-19-triggering-event-reassessing-risk-and-adequacy-data-privacy-and-security-0