BMA ADVOGADOS

Digital compliance and cybersecurity in crisis management in the public and private sectors

31.03.2020 4 min read

Authors

Anna Carolina Malta Spilborghs

José Guilherme Berman

In times of crisis, regardless of the cause, it is essential to reinforce digital compliance efforts, especially cybersecurity and digital governance. Reports are already circulating in the media that predict or confirm an increase in cyberattacks, just at a time when society must rely more than ever on digital communication and digital solutions.

Taking to heart the saying that an ounce of prevention is worth a pound of cure, BMA's Compliance, Investigations and Enforcement specialists put together a list of tips to help companies strengthen their compliance measures, directed to the use of technology in distributed work, home-based work and other uses of digital environments as substitutes for regular business operations. If these measures have not already been implemented by companies' compliance departments, they should be – as soon as possible given the operational reality now facing Brazilian businesses.

1. **Cybersecurity and electronic devices used for work:** Update all apps and software, both operating systems and anti-virus and security apps in general, on all devices used for work and to connect to corporate information;
2. **Remote work policies:** Review or establish your organization's policy on remote work and the use of technology for work-related and corporate purposes. Everyone has to take extra care when working from home, especially (a) to avoid accidental disclosure of confidential information on social networks, (b) when expressing opinions on social networks about the current scenario, particularly when that opinion conflicts with action taken by the company, (c) when sharing any type of content that could expose the company or its personnel in the phase of adaptation to remote work. All of a company's collaborators should be aware that all information circulated among collaborators must be kept confidential;
3. **Ongoing awareness campaigns:** Conduct awareness and compliance campaigns weekly or every two weeks, stressing how important it is for collaborators to use extra caution when opening e-mails and navigating on the internet, because of the significant increase in phishing attacks (false e-mails and websites that appear to be genuine, designed to steal information like log-ins, passcodes, and bank information among other sensitive information and accounts) that rely on news and information related to COVID-19;
4. **Safety when navigating on the internet and using on-line services:** Additional care should be taken when making on-line purchases and banking on-line. The migration to on-line shopping and banking has been sizeable because of the social distancing measures implemented

around the world;

5. **Review passcodes and accounts:** Reinforce how important it is for everyone in your organization to use complex passwords, including two-step verification, on all personal and corporate electronic devices, if possible.
6. **Task force operations to support cybersecurity and strategic areas:** Another recommendation for companies' compliance teams is to work in task force configurations in partnership with the company's Information Technology and Security group, Operations, Finance, and senior management to review the company's entire digital governance structure, with special emphasis on cybersecurity, business continuity, and protection of knowledge and information;
7. **Hardware and connection security review:** Remind your collaborators to change their internet router passwords and update equipment firmware in order to strengthen the security of distributed connections. Ask your organization's IT group to provide step-by-step instructions to all collaborators, and remember that the organization does not have control over the connections its collaborators use for work. Whenever possible, offer VPN services, which encrypts users' connections to the internet.

In addition, it is important to review or create protocols on the following matters:

- **Business continuity:** Establish or review crisis management and contingency plans, along with plans for business continuity;
- **Treatment of confidential information:** Establish a policy and rules on the care to be taken when dealing with sensitive information in audio and video calls, and the prohibition against disclosing confidential information to family and friends;
- **Review compliance rules:** With remote work now the norm, it is essential to review ways of determining whether collaborators are adhering to the organization's compliance program and related rules and policies;
- **Monitor interaction with public agents:** Given the new dimensions of interaction between companies and public authorities resulting from cooperative initiatives to combat COVID-19, special attention should be given to the constant change in state and municipal legislation that can affect businesses in the private sector, and protocols for interaction with

the civil service and its representatives should be reviewed; and

- **Review Emergency Costs and Expenses:** In times of crisis, many costs and expenses are claimed to be emergency-related. It is important to review such costs, ideally in real time but in any case as soon as possible, in order to prevent surprises in the form of potential frauds and abuses of emergency funds. In addition, when emergency spending is necessary, all documentation for approval and monitoring of the expenditures should be included in expense management systems or stored for later review and analysis.

BMA's Compliance team is available to provide advice and guidance on which measures should be prioritized when it is impossible to implement all measures, and, through remote work arrangements, help clients act on compliance and digital security issues without undermining efforts directed to priority initiatives.

Image: rawpixel.com/ Freepik

› PROFESSIONALS

Professionals who combine legal insight and market perspective


Anna Carolina Malta Spilborghs


José Guilherme Berman