Data, security and risk: taking a standards-based approach

Across the globe, the pandemic has made significant social and economic impacts, which has caused long-term changes to working culture and consumer behaviour, and has heightened other serious risks for industry.

Amongst these risks, cybersecurity has proved to be one to look out for. During the past few months, reports of cybersecurity incidents and attempted data breaches have increased drastically.

The reoccurring lockdowns and home working have meant that individuals, businesses and institutions are relying more heavily on digital networks for all aspects of communication and operation. As usual, cybercriminals have been quick to try and take advantage of this greater vulnerability.

Unfortunately for a large organization with a regional, national or even international reputation, a single information security incident can have a significant impact on brand perception and consumer trust. Once data is lost or stolen, even if the breach is caused by a mistake the consequences can be long-lasting.

Organizations risk financial loss, fines and reputational damage.

Operations are often disrupted too, and if any intellectual property is compromised, competitors may be able to access critical information to erode a brand's competitive edge.

A standards-based strategic approach to information security protocols pays dividends – particularly in uncertain times. It helps larger organizations secure varying operational and geographical priorities, as well as ensuring that an increasingly dispersed and home-based workforce becomes a cybersecurity advantage, rather than a risk.

Executives can use standards to better understand information security risk levels, consulting BS EN ISO/IEC 18045:2020, which outlines a methodology for evaluation, and BS EN ISO/IEC 15408-3:2020, for an evaluation criteria and assurance components for IT security.

With benchmarking complete, executives can use BS EN ISO/IEC 27001:2017 to design a bespoke information security management policy.

This standard provides a systematic framework to counter an array of evolving cybersecurity threats. Importantly for larger companies, it highlights the requirement for a holistic approach to information security.

Documented, company-wide policies based on international standards will enable leaders to instil the right awareness and vigilance amongst employees. They should prioritize education and training for all, regardless of department.

Other standards in the ISO 27000 series are also very helpful – particularly when ensuring that staff understand their responsibilities. BS EN ISO/IEC 27002:2017, for example, provides a code of practice for information controls which is useful for corporations with homeworking teams across multiple locations.

With a strong foundation in place, executives can then consult BS EN ISO/IEC 27014:2020 for guidance on key concepts, objectives and processes for the top-level governance of information security. It sets out roles and responsibilities for executive management and boards of directors, helping them to make timely decisions in support of their business objectives.

Meanwhile, the proper storage of organizational, customer and stakeholder data are a vital consideration for legislative compliance and reputational safety. Cloud-based services are ubiquitous, and every company should have specific storage policies.

Thankfully, there are some well-established standards for managers to use in this area. BS ISO/IEC 27017:2015 provides enhanced controls for both cloud service providers and their customers. This is important when defining precise roles and responsibilities and ensuring that all cloud storage relationships are as secure as possible.

Legislation around personal data, and its secure management, has made the headlines in recent years, with the introduction of regulations like GDPR in Europe. BS ISO/IEC 27701:2019 provides a common set of concepts with which organizations can tackle personal data protection, and better demonstrate compliance. The standard works as a privacy extension to ISO 27001 and 27002, outlining how to establish and run a privacy information management system (PIMS).

Beyond this, modern supply chain operations demand secure information exchange and storage capabilities to maintain trust and confidence between partners. Organizations can use BS ISO/IEC 27036-1:2014 to provide an overview for information security within supplier relationships, and BS ISO/IEC 27036-3:2013, which outlines related guidelines for supply chain security.

All the standards we've highlighted here underscore the importance of frequent monitoring, benchmarking and continued improvement. Effective information security is an ongoing process and no organization can afford to become complacent – the nature and complexity of external threats are constantly evolving.

Certification to international standards demonstrates an organizational commitment to the highest levels of information security. This is vital in the current climate of uncertainty and tentative economic recovery.

A standards-based approach enables companies to mitigate risk and reduce the overall impact in the event of any incident.

Summary

- A standards-based strategic approach to information security protocols pays dividends – particularly in uncertain times.

- Executives can consult BS EN ISO/IEC 18045:2020 which outlines a methodology for evaluation, and BS EN ISO/IEC 15408-3:2020, for an evaluation criteria and assurance components for IT security.
- BS EN ISO/IEC 27001:2017 allows managers to design a bespoke information security management policy.
- BS EN ISO/IEC 27002:2017provides a code of practice for information controls, particularly helpful for corporations with homeworking teams across multiple locations.
- Consult BS EN ISO/IEC 27014:2020 for guidance on key concepts, objectives and processes for the top-level governance of information security.
- BS ISO/IEC 27017:2015 provides enhanced controls for both cloud service providers and their customers.
- BS ISO/IEC 27701:2019 provides a common set of concepts with which organizations can tackle personal data protection, and better demonstrate compliance.
- Organizations can use BS ISO/IEC 27036-1:2014 to provide an overview for information security within supplier relationships, and BS ISO/IEC 27036-3:2013, which outlines related guidelines for supply chain security.
- Effective information security is an ongoing process, and no organization can afford to become complacent – the nature and complexity of external threats are constantly evolving.
- Certification to international standards demonstrates an organizational commitment to the highest levels of information security. It enables companies to mitigate risk and reduce the overall impact in the event of any incident.

Find out how BSI protects your people, information and reputation: https://www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/