Cybersecurity: getting your house in order

One of the more significant second-order effects of the recent pandemic has been the widespread increase in reported cybersecurity incidents and attempted attacks. The FBI, for example, reported a three to four-fold increase in cyber threat reports in April, and the UN highlighted a 600% increase in malicious emails by the end of May.

Further, national lockdowns increased reliance on digital systems and communication technology across the industrial, social and educational realms. Malignant actors all over the world have grasped the opportunity to exploit this increased vulnerability, as well as the lack of adaptive awareness and training in the area.

Regardless of whether a security breach is caused by human error or external agents, failures can have severe and long-lasting consequences. These include financial losses, fines and reputational damage. Day-to-day operations can be disrupted or halted. Also, if intellectual property is compromised, businesses risk losing their competitive edge.

Taking a standards-based approach to organizational cybersecurity is the best strategy in these difficult times. It enables companies to maintain systems of defence and risk mitigation, as well as reduce damage and overall impact in the event of an incident.

For example, ISO 27001 allows organizations to create and document a tailored information security management policy. It provides a systematic approach to counter an array of evolving cybersecurity threats. ISO 27002, meanwhile, provides a code of practice for information security controls.

ISO 27001 also highlights the requirement for a holistic approach to information security, which prioritizes education and training for all employees, regardless of role. Documented policies based on international standards will help leaders instil company-wide awareness and vigilance.

This is particularly important for groups spread across multiple locations or countries, to ensure all staff understand risks and responsibilities, and embrace specific controls in their everyday activities. With many companies working entirely from home the importance of this approach becomes clear.

Another security area which has been intensified with widespread dispersed working is personal device use. Although smaller firms can more easily quantify and control how staff work on private devices, it can prove difficult for larger corporations. For this reason, it is vital to include personal device rules in all cybersecurity policy documentation.

When it comes to governing information security within an organization, businesses can consult ISO 27014 for guidance on key concepts and principles. The standard helps managers make timely decisions regarding information security issues in support of their business objectives.

Cloud-based services and storage policies are an important operational consideration for every modern organization. ISO 27017 provides enhanced controls for both cloud service providers and their customers. It clarifies roles and responsibilities to ensure that cloud services are as secure as possible. Further to this, ISO 27701 helps organizations protect the personal information they handle.

International standards also introduce frequent measurement, benchmarking and continued optimization, underlining the fact that cybersecurity is always an ongoing process and is never complete.

Because the nature and complexity of external threats are constantly evolving, so too must organizational defences.

As a result, it's advisable to set cybersecurity as a standing agenda item at board meetings, both to underline its strategic importance and encourage an ongoing and open dialogue. Further to this, frequent internal communications and reminders should be used to keep staff informed and engaged.

The supply chain disruption caused has by the coronavirus pandemic has been felt around the world, affecting businesses in every sector. As well as general supply chain security standards, organizations can draw upon more specific guidance. For example, ISO 27036-1, which provides an overview for information security within supplier relationships, and ISO 27036-3, which outlines related guidelines for supply chain security.

Many forward-thinking companies also run phishing simulations and other training scenarios to assess specific training requirements and risk areas. For further help with benchmarking threat levels, executives can consult ISO 18045 for a methodology for security evaluation, and ISO 15408-3, which provides evaluation criteria and security assurance components for IT security.

Certification to international standards will demonstrate to partners, stakeholders, investors and customers your business is committed to maintaining the highest levels of information security. This is an even more important consideration in the current climate of uncertainty and tentative economic recovery. By strengthening security measures and educating staff on cybersecurity, you can ensure your business moves forward successfully in 2020 and beyond.

Summary:

- One of the more significant second-order effects of the coronavirus recent pandemic has been the widespread increase in reported cybersecurity incidents and attempted attacks.
- Information security failures can have severe and long-lasting consequences. A standards-based approach to organizational cybersecurity is the best strategy in these difficult times.
- ISO 27001 allows organizations to create and document a tailored information security management policy. ISO 27002 provides a code of practice for related controls.
- Another security area which has been intensified post-coronavirus is personal device use. It's vital to include related rules in all cybersecurity policy documentation.
- When it comes to governing information security within an organization, businesses can consult ISO 27014 for guidance on key concepts and principles.
- ISO 27017 provides enhanced controls for both cloud service providers and their customers. ISO 27701 helps organizations protect the personal information they handle.
- Cybersecurity is an ongoing process. As such, it's important to set cybersecurity as a standing agenda item at board meetings and engage in frequent internal communications on the issue.
- To protect supply chain information consult ISO 27036-1 for an overview of information security within supplier relationships and ISO 27036-3 which outlines related guidelines for supply chain security.
- For further help with benchmarking threat levels, executives can consult ISO 18045 for a methodology for security evaluation and ISO 15408-3 for evaluation criteria and security assurance components for IT security.
- By strengthening security measures and educating staff on cybersecurity, you can ensure your business moves forward successfully in 2020 and beyond.

For more information on cybersecurity visit:

www.bsigroup.com/en-GB/our-services/Cybersecurity-Information-Resilience/