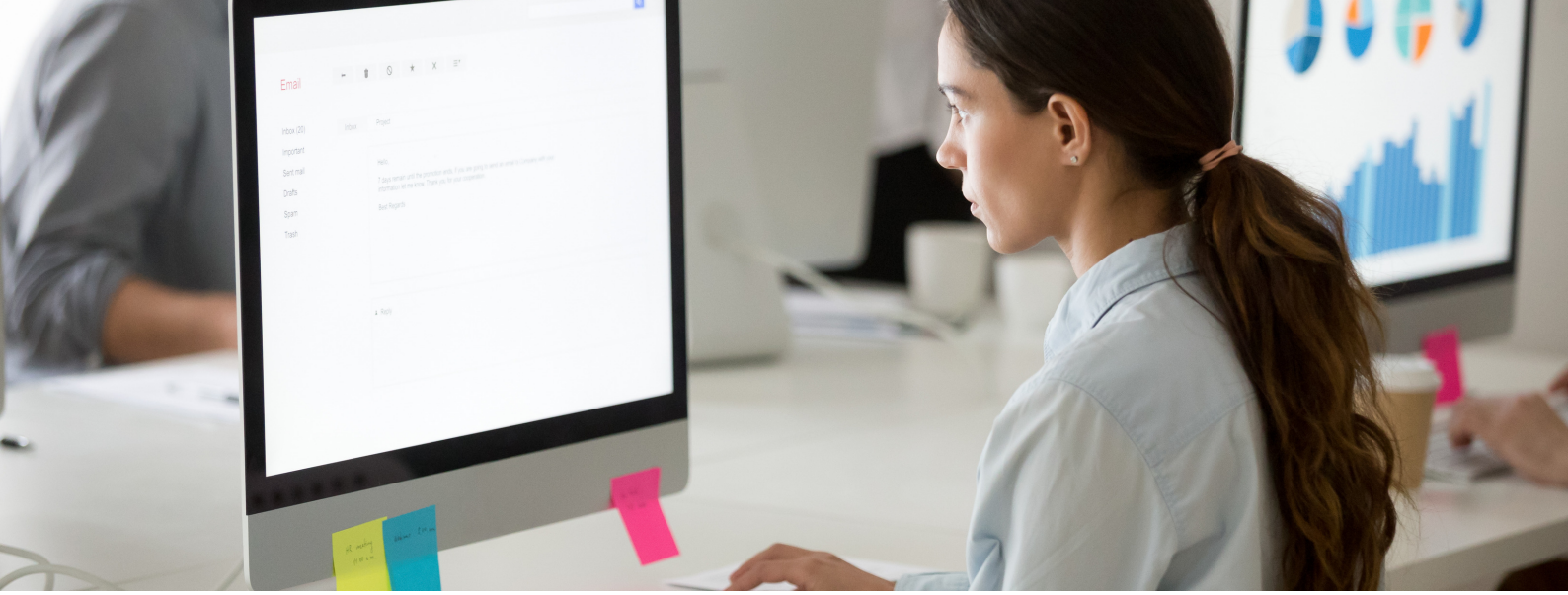

Managing your cybersecurity risk profile

Every organization runs on data - information it generates internally, receives externally, and stores for the short or long-term. Whether this data relates to its operations, partners, or customers the costs and consequences of a breach or related security incident have never been higher, from both a financial and reputational perspective. Taking a standards-based approach to cybersecurity helps build resilience for the long term.

With new information continually generated corporations must stay in control of storage, access security and management processes. Indeed, one of the most important developments within organizational governance in recent years is that cybersecurity is no longer the sole preserve of technical specialists in the IT department. It's a mainstream, strategic business issue which must be prioritized accordingly. Despite this, many organizations are still not doing enough to protect themselves.

According to a 2019cybersecurity study conducted by IBM, three-quarters of businesses do not have a plan in place to respond to a cybersecurity incident. This is even more concerning in light of research published by the Department for Digital, Culture, Media and Sport, suggesting that every data breach or cyber incident results in losses of £4,180 on average - up from £3,160 in 2018 – for businesses.

Standards help executive teams act with confidence to build significant resilience against cyberattack and data breaches – enabling better protection for customers, partners and stakeholders. They introduce processes which help guard against both deliberate and chance incidents, as well as assisting with legislative compliance.

Giventhe huge volumes of data generated and processed by most corporations, information security has become a key reputational consideration. What's more, fines for proven mismanagement under the general data protection regulation (GDPR) are significant, and the number of famous organizations and brands receiving penalties is steadily growing.

Corporate teams can use ISO/IEC 27001 to design and implement an overarching information security management system, while ISO IEC 27552 will focus on improved privacy controls when it launches later in 2019.

Closely related is the issue of how this information and data is stored, given how most large organizations use cloud services for most, if not all, of their requirements. Implementing a management teams make the right choices when selecting cloud service

providers, as well as manage the resulting storage arrangements. ISO/IEC 27017 outlines guidelines for information security controls around the provision and use of cloud services.

Modern flexible, and home-based, working practices present new risks related to employees using their own devices for work tasks. Some companies now maintain a bring your own device (BYOD) system. These situations require the right awareness and understanding from staff when it comes to their security responsibilities. Creating a clear policy, in line with ISO 27001 requirements, is the best way to reduce risks associated with BYOD arrangements.

Another significant consideration for large organizations employing hundreds or thousands of staff is the human error factor - often cited as a common cause of cybersecurity incidents. Employees make mistakes and misjudgements but can also be exploited by criminals who understand how vulnerable busy, distracted people can be.

Management teams can use standards to optimize security-awareness training and strengthen the cybersecurity chain, empowering employees to become an organization's best protection against attack.

It's also worth considering ongoing internal communications and reminders on the subject, as well as running phishing simulations and other training scenarios to assess specific training requirements and risk areas.

Using this information, executive teams can better tailor training plans to individual needs. The information security standard ISO/IEC 27001 helps small businesses create and structure training in accordance with international best practices, as well as define responsibilities in the event of a breach.

Given the consequences of failing to comply with regulations like GDPR, businesses can't be too careful when it comes to cybersecurity. Taking a standards-based approach helps organizations implement a robust approach to managing information security and building resilience. Certification to key standards inspires widespread trust in your business, demonstrating to customers, suppliers and the market that you can handle information securely.

Summary:

- Standards help organizations act with confidence to protect themselves, their customers and partners – as well as assisting with legislative compliance.
- Management teams can use ISO/IEC 27001 to design and implement an overarching information security management system, while ISOIEC 27552 will focus on improved privacy controls when it launches later in 2019.
- Any information security management policy based on ISO 27001 principles should also cover the use of personal devices for work tasks, as well as reduce the likelihood of humanerror causing a cybersecurity incident – helping to turn employees into an effective human firewall.
- Data storage is also important. ISO/IEC 27017 helps executive teams select cloud service providers, as well as manage the resulting storage arrangements.
- ISO/IEC 27001 also helps businesses structure cybersecurity training in accordance with international best practices, as well as define responsibilities in the event of a breach.
- A standards-based approach helps managers implement a robust approach to information security and cyber resilience. Certification to key standards also inspires greater external trust in the business

For more information on our business improvement standards, visit:

www.bsigroup.com/standards