How to tackle today's IT security risks

Based on an ISOFocus article

Industry experts estimate that annual losses from cybercrime could rise to USD 2 trillion by next year. With countless new targets added every day, especially mobile devices and connected “things”, a joined-up approach is essential.

The attraction of cybercrime to criminal hackers is obvious: tangled webs of interactions, relatively low penalties, disjointed approaches on money laundering and potentially massive pay-outs. The key is preparation. Seeing vulnerabilities, and resilience, in terms of interactions with overall management systems is where information security management systems (ISMS) standard ISO/IEC 27001 comes in.

This standard is the flagship of the ISO/IEC 27000 family of standards, which was first published more than 20 years ago. Since its creation, it has been constantly updated and expanded to include more than 40 International Standards covering everything from the creation of a shared vocabulary, risk management, cloud security to the forensic techniques used to analyse digital evidence and investigate incidents.

These standards are not only about helping to manage information security but will also help to identify and bring criminals to justice. For example, ISO/IEC 27043 offers guidelines that describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation. The key is preparation and seeing vulnerabilities.

Staying ahead of the game

Keeping this family applicable to the needs of businesses small and large through a process of constant evolution is a serious responsibility for international standards development organizations ISO and IEC. It’s in large part thanks to the contribution of people like Prof. Edward Humphreys; a specialist in information security and risk management with more than 37 years of experience in consulting and academia, who chairs the working group responsible for developing ISMS, that it remains one of the most effective risk management tools for fighting off the billions of attacks that occur each year.

“It’s true that risks that threaten information, business processes, applications and services are continually evolving. ISO/IEC 27001 is a continual improvement standard, which means the built-in risk management process allows businesses to keep up to date in their fight against cybercrime." Says Prof. Humphreys.

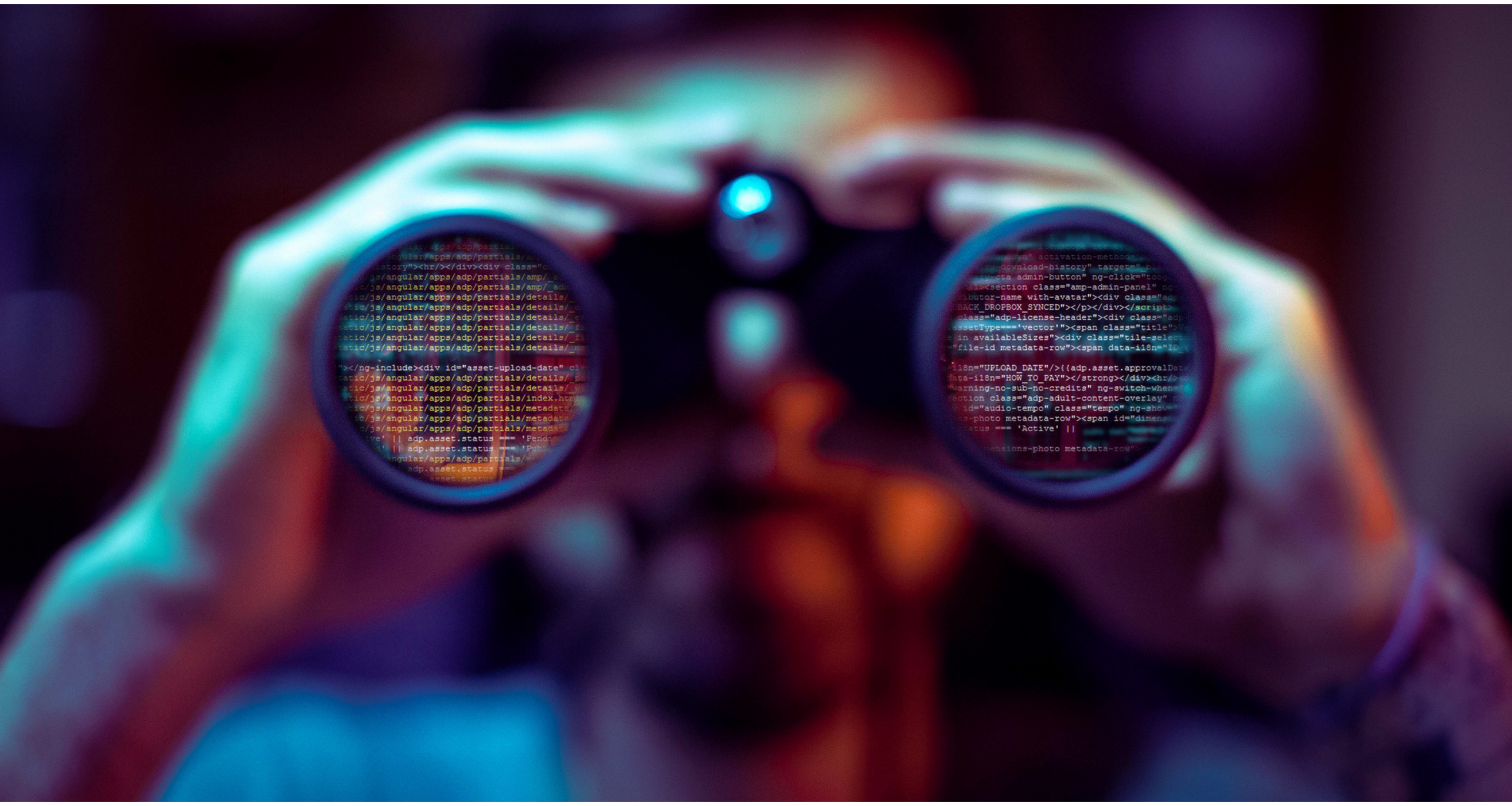
In fact, according to Prof. Humphreys, the continual improvement aspect of ISO/IEC 27001 means that an organization can assess its risks, implement controls to mitigate these, and then monitor and review its risks and controls, improving its protection as necessary. In that way, it's always on the ready and prepared for attacks: " If used properly, ISMS enable the organization to keep ahead of the game, responding to the evolving risk environment that the Internet and cyberspace present."

From threats to opportunities

At the business level, it remains a formidable task to model and mitigate threats from all conceivable angles. There's a clear need to use a conceivable angles. There's a clear need to use a unified, integrated security system across the whole business and, given the complexity of interrelationships, it may be unclear whether ISMS could apply to small and medium-sized enterprises (SME).

"ISMS are applicable to all types of organization and all types of business activities, including those of SMEs. Many SMEs are part of supply chains, so it's essential that they are in control of, and manage, their information security and cyber-risks in order to protect themselves and others." Prof. Humphreys explains that a business's obligations are typically defined in service-level agreements, contracts between partners of the supply chain that detail service obligations and requirements and establish legal liabilities, and that ISMS often form an integral part of such agreements.

The upsides for social and economic development are enormous: the internet brings



global reach to growing numbers of previously isolated individuals and communities. However, a proven and prudent approach such as ISMS is needed to mitigate the downsides. As Prof. Humphreys states, "a cyber-attack on one part of the supply chain could disrupt the whole of the chain" and the impacts can reach way beyond your own business, or even your direct clients. That's as true for artisan toymakers from Bali as it is for government national health services in Europe.

The right to privacy and the need for confidence

When privacy, finances, individual or corporate reputation are threatened, it undermines confidence and impacts our behaviour, both online and in real life. The role of the ISO/IEC 27000 family in allowing us to continue to advance is paramount. With many reasons to feel anxious as almost every aspect of our lives becomes digitized, it's reassuring to know that there's a family of standards to count on for information security management systems, and a global group of experts like Prof. Humphreys working to keep us one step ahead.

Find out more about cybersecurity with BSI

Call **1300 730 134**
or visit **bsigroup.com/en-au**