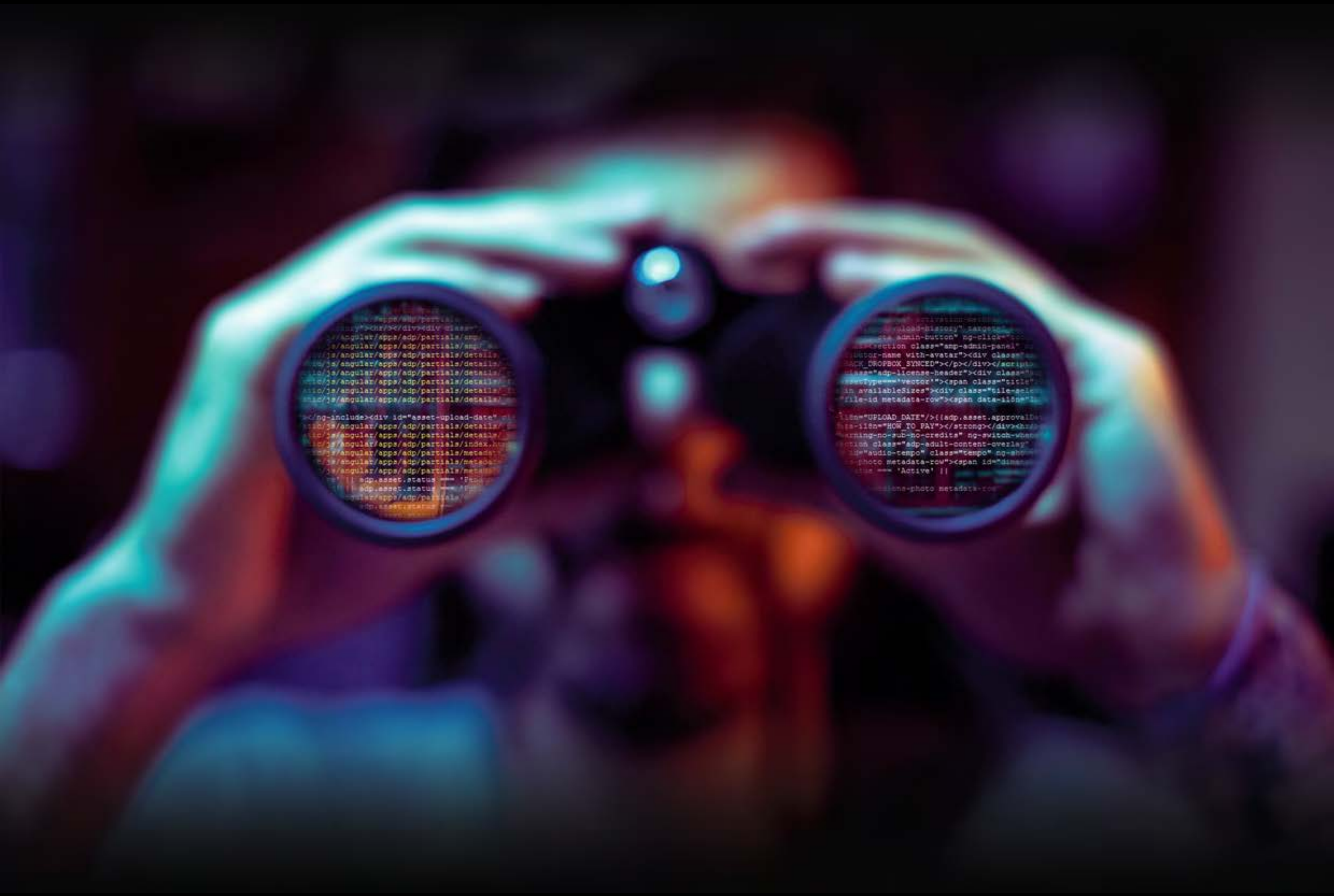
bsi.

...making excellence a habit.™



understanding your CYBERSECURITY RISK

How standards can help you protect your organization

Understanding your cybersecurity risk

Cybersecurity is an issue for every organization across the world, regardless of size or focus. Over the past decade it has moved from a technical specialism to a mainstream concern for individuals, businesses and government.

Despite this, many organizations are still not doing enough to protect themselves. According to a 2019 cybersecurity study conducted by IBM, which surveyed more than 3,600 security and IT professionals from around the world, three-quarters of businesses do not have a plan in place to respond to a cybersecurity incident.

Also, a significant proportion (45%) of companies that do have such a process in place don't test it regularly, or even at all, making it impossible to keep up to date and exposing vulnerabilities in a fast-moving environment. This is no longer just an issue for IT professionals – in today's world, all organizations and their employees must take responsibility for digital security.

From the biggest government department shielding critical infrastructure 24 hours a day, to a microbusiness looking after its customer data, the right awareness and knowledge is needed to guide everyone in the workplace.

The most effective way to improve cybersecurity is by using internationally recognized standards to introduce processes which protect against both deliberate and chance incidents.

Standards help companies improve their cybersecurity levels in a number of ways – from informing new processes to shield your company to delivering more effective employee training, as well as introducing better data protection and assisting with legislative compliance

So, what are the key areas of cybersecurity risk for most companies, and which standards can help organizations address them?

Data privacy

Every organization, public or private, runs on data – its own and that relating to its employees and partners, as well as customer or user data.

With new information generated every second, it's imperative to stay in control of how it's stored, who can access it and how it's managed.

Also, with GDPR now firmly in place, the financial consequences for a significant data breach are very serious – not to mention the potential reputational damage.

Businesses can use ISO/IEC 27001 to implement an overarching information security management system, while ISO/IEC 27701 focuses on improved privacy controls.

Cloud security

Cloud computing is another area which has transformed the way that most organizations store data, in just a few years.

Although many businesses initially felt cautious about transferring critical data and functionality to the cloud, it has now become commonplace, with standards playing a key supportive role.

There are a number of standards that help organizations make the right choices when selecting cloud service providers, and then control the resulting storage arrangements.

One of the most relevant is ISO/IEC 27017:2015 which outlines guidelines for information security controls around the provision and use of cloud services – covering implementation as well as management processes.

PROTECTION AGAINST CYBERASSAULTS

BS 31111

Cyber risk and resilience. Guidance for the governing body and executive management

ISO/IEC 27032

Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27033

Information technology – Security techniques – Network security

ISO/IEC 27034

Information technology – Security techniques – Application security

DATA MANAGEMENT AND CLOUD STORAGE

ISO/IEC 27701

Privacy Information Management – Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002. Requirements.

ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Bring your own device (BYOD)

With the rise of flexible and home-based working, many more employees are working remotely as opposed to gathering in a single location.

A lot of companies use a bring your own device (BYOD) system which sees staff using personal mobile devices for work activities. Although this can improve efficiency it also adds a layer of risk, since these devices are connected to corporate networks.

Employee awareness and understanding of BYOD security responsibilities are critical to organizational risk.

Creating a clear policy for all staff, in line with ISO/IEC 27001 requirements, is the best way to mitigate security risks associated with BYOD arrangements. We also recommend referring to BS ISO/IEC 38500, which provides guidance for IT governance.

PROTECTING COMPANY INFORMATION

ISO/IEC 27001

Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002

Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003

Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27005

Information technology - Security techniques - Information security risk management

BS 7799-3

Information security management systems. Guidelines for information security risk management

Human error

Recent research puts human error as the top cause of cybersecurity incidents.

Criminals know to exploit individuals, rather than systems, because they understand just how vulnerable busy, distracted people can be – especially those who might not have cybersecurity front of mind.

However, standards put security-awareness training at the forefront to help strengthen your cybersecurity chain, empowering employees to become a ‘human firewall’. Using phishing simulations and knowledge assessment, organizations can accurately assess specific training requirements, and current risk – ideally at the individual user level.

Using this as a baseline, companies should then tailor plans to an employee’s needs. The information security standard ISO/IEC 27001 helps companies create and structure training in accordance with international best practices, as well as define responsibilities and protocols in the event of a breach.

You can get individual copies of every standard in our shop, or access and manage your collection of cybersecurity standards packages using British Standards Online (BSOL).

BSOL
Standards Online

The reassuringly easy way to work with standards

BSOL is a simple online tool that gives you instant access to the standards you need, making life a lot easier. It's easy to build your own database of relevant standards. Then you can find what you need fast and stay right up to date – so you can avoid costly errors and work with confidence.

Know you're covered

Save time

Manage all your standards in one place. You can access ISO, EN, BS ASTM and IEC standards through BSOL – and it takes only seconds to search.

Save money

Make standards even better value for money. Using BSOL gives you large savings on your traditional standards spend.

Miss nothing

Get an alert whenever a standard changes and understand the significance immediately. Then view the differences to key standards, so you can track exactly how they've changed.

Reduce risk

Track past, present and future changes. With access to historic and emerging standards, you can see the guidance that informed previous decisions, as well as changes that could shape your future moves.

Fit the way you work

Tailored to you

Subscribe only to the standards you need, use pre-built modules or build personal collections.

Full flexibility

You can still access every standard in the system and update your choices at any time.

Easy monitoring

Monitor which standards your users are working with, and easily spot gaps or overlaps.

Free and unlimited training

Our training team are here to give you extra support if you need it.

Make life easier with BSOL.

Get a quote or find out more at bsigroup.com/bsol.
Or call +44 (0)345 086 9001.

...making excellence a habit.™