Digital Security.

Building a strategic response to cyber risk.

Combatting cyber risk in business is no longer the exclusive concern of the information security team. It has fast become a regular agenda item at Board meetings around the world, due to the wide-ranging financial and reputational implications that a data breach can have to an organization.

Media headlines containing "Cyber Attack!", "Severe Data Breach" and "Hackers Hit..." are seen with increasing regularity and the implications for affected organizations can be costly.

Counting the cost

The three main causes of a data breach are malicious or criminal attack, a system glitch or human error[1]. The costs of a data breach can vary according to the cause and the safeguards in place at the time of the incident, but a recent UK Government survey showed that the average cost of a data breach has more than doubled between 2014 and 2015 to an average of between £1.46m-£3.14m for large organisations[2].

In addition to the expenses of responding to cyber-attacks, companies find they must spend heavily to regain their brand image and acquire new customers. Additionally, senior executives are acutely aware of the impact that a tarnished reputation and associated loss of customer loyalty can have to the bottom line.

91% of large organizations had a security breach in 2015

50% of worst security breaches caused by inadvertent human error

28% of the worst security breaches were caused partly by senior management giving insufficient priority on security

15% of large organisations had a security or data breach in the last year involving smartphones or tablets

16% were attacked by an unauthorised outsider in the last year.

Source: HM Government 2015 Information Security Breaches Survey.

Customer confidence

Whether your customer is a business or consumer, it's time to question how confident they feel about the security of their information. What steps are you taking to reassure customers around data integrity and digital security? Are you standing out as an organization that takes excellence in cyber security to the next level?

[1]*Source: 2014 Information Security Breaches Survey – Department for Business Innovation & Skills.*

[2]*Source: HM Government 2015 Information Security Breaches Survey.*

bsi.

...making excellence a habit.™

Digital certification standards and beyond

At BSI we have experts with depth of commercial and technical understanding who will help you to look at the bigger picture. Together, we will explore how your business can ensure it does everything in its power to reduce cyber risk, build trust with customers and help differentiate itself from competitors in a nervous market.

We can help your organization to demonstrate industry compliance and best practice; providing evidence that your systems are reliable, secure and can demonstrate the highest levels of quality. As part of your solution we will consider compliance to ISO/IEC 27001, the internationally recognized best practice framework for an information security management system; the government-backed Cyber Essentials & Cyber Essentials Plus schemes and CSA STAR Certification or ISO/IEC 27018 which address specific cloud security concerns.

Additionally, BSI Kitemark certification schemes for **Digital Security** and **Secure Digital Transactions** may be suitable for organizations that wish to demonstrate they go above and beyond these standards.

About BSI Kitemark™

In 2015 an independent consumer survey showed that the BSI Kitemark is associated with rigour; consumers know products and services displaying the BSI Kitemark are tried and tested therefore consumers trust products and services displaying the BSI Kitemark.

What supports this?

67%
of consumers **have awaremess** of the BSI Kitemark.

BSI Kitemark could command **price premiums** up to 26%

60%
of consumers **willing to pay more** for a product displaying a BSI Kitemark.

Cyber Essentials

Is a cyber-security standard that identifies the security controls organisations must have in place within their IT systems to have confidence that they have a basic level of cyber security and are mitigating the most common internet-based threats. BSI is CREST-accredited certifying body for the Cyber Essentials scheme. Since October 2014, Cyber Essentials has been a minimum requirement for bidding on some government contracts and is becoming a mandatory requirement for many other contracts handling sensitive information or moderate to high-level risk.

ISO/IEC 27001

The world's most widely recognized information security management system that enables organizations to effectively secure all financial and confidential data and prove to customers and stakeholders that security is paramount to the way they operate. It helps identify the risks to your important information and put in place the appropriate controls to help reduce the risk.

Digital Security Kitemark

The Digital Security Kitemark builds on the principles of the Secure Digital Transactions Kitemark with an expansion of scope, measuring the security of the following areas: Network, Application, Infrastructure, Operations, IS Risk Management and Security Management. This requires the organization to cover one or all of these under ISO/IEC 27001 and have considered the risks in Appendix A of ISO/IEC 27001. These areas are tested by a qualified CREST 10,000 hour tester for vulnerabilities, using methods such as the CVSS (Common Vulnerability Scoring System) to calculate the results.

Above and beyond required standards

CSA STAR Certification for Cloud

Following the rise in the adoption of cloud computing services and the new risks in this area, BSI has worked with the Cloud Security Alliance (CSA) to develop CSA STAR Certification to provide the extra reassurance that cloud specific security issues are being addressed and managed effectively.

Secure Digital Transactions Kitemark

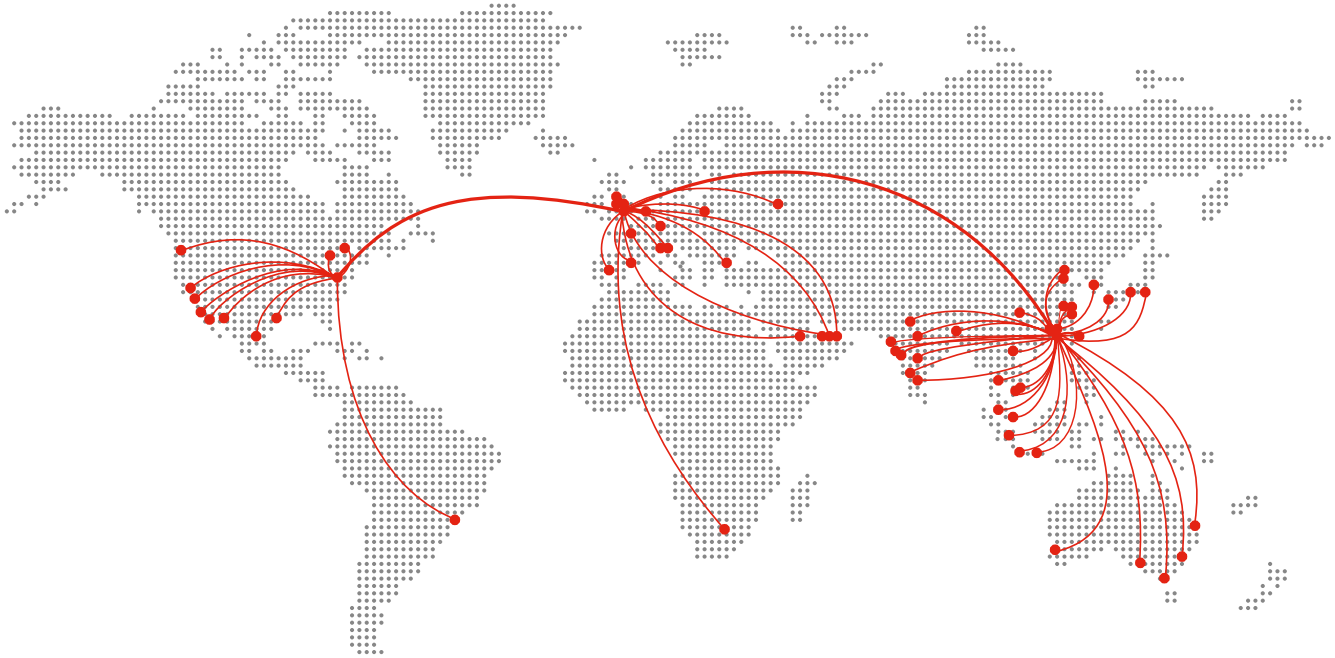
The BSI Kitemark for Secure Digital Transactions requires a website or application to undergo rigorous and independent testing against OWASP (Open Web Application Security Project) standard ASVS V2.0 (Application Security Verification Standard) as it transacts from a device through the web to a server, ensuring it has the security controls in place for the financial and/or personal information it is handling. Producers of any website or application can reassure customers of its security by displaying the Kitemark in their marketing materials. Assessment involves organizations achieving and maintaining certification to ISO/IEC 27001 for the parts of the business that handle confidential data as well as undergoing rigorous internal and external penetration test which scan for vulnerabilities and security flaws.

ISO/IEC 27018

The standard gives guidance for cloud service providers that process Personally Identifiable Information (PII) and aims to address the risks of public cloud computing and to help build confidence in public cloud computing providers. It offers a set of controls which Cloud Service Providers (CSPs) need to implement in order to address the specific risks and gives guidance on what CSPs need to achieve in terms of contractual and regulatory obligations.

Cyber Essentials Plus

This encompasses all of the elements of Cyber Essentials along with an internal security assessment of end-user devices. This is a more thorough assessment conducted by BSI, who is a CREST-accredited certifying body, and will test that the individual controls have been correctly implemented and recreates numerous attack scenarios to determine whether your system can be compromised. This is a snapshot of your organisation's security at the time of assessment and does not provide assurance that the controls will continue to be implemented correctly or that your system is able to defend against sophisticated or persistent attacks.



About BSI

We are the business standards company that equips businesses with the right tools and solutions to turn best-practice standards into habits of excellence. With over 3,000 staff worldwide, we help our clients drive performance, manage risk and grow sustainably.

Founded in 1901, we were the world's first National Standards Body. Now over a century later, we're globally recognized as a champion in best practice. We have been and still are responsible for originating many of the world's most commonly used management systems standards and publish nearly 2,700 standards every year. These standards are developed to address the most pressing issues of today, such as clear billing, energy management, disability access, nano-technology and more. They also cover various industry sectors, including Aerospace, Automotive, Built Environment, Food, Healthcare and IT.

All our standards are underpinned by a collaborative and rigorous approach perfected over decades. We always work closely with industry experts, government bodies, trade associations, businesses of all sizes and consumers to develop standards that drive excellence.

We currently work with over 80,000 clients in 172 countries worldwide to help them adopt and cultivate continuous habits of best practice. We also train all our clients and provide them with practical implementation guidance, as well as a comprehensive suite of compliance tools. And to ensure our clients get the very best service, we're also independently assessed and accredited globally by ANAB (ANSI-ASQ National Accreditation Board) and 26 other accreditation bodies throughout the world, including UKAS (United Kingdom Accreditation Service).

Our reach is global and we play a key role within the International Organization for Standardization (ISO). As one of the founding members, we help make sure international standards developed address today and tomorrow's business and societal needs, while delivering real benefits to an organization and all its stakeholders.

Speak to one of our experts today or visit our website for more information.

Call: +852 3149 3300
Email: hk@bsigroup.com or
visit: bsigroup.com/en-HK

bsi.