bsi.

...making excellence a habit.™

controlling VULNERABILITY

The role of standards in mitigating cybersecurity risk

Foreword

“BSI is dedicated to promoting best practices to meet a constantly evolving cybersecurity challenge. Working with organizations of all sizes in 182 countries worldwide, we help drive compliance, reduce risk and increase resilience.”

Howard Kerr, Chief Executive, BSI

Introduction

It’s thought that students at a Chicago high school were responsible for the first recorded network hacking incident. In 1967, members of the Evanston Township High School computer club gained access to IBM’s APL network system. They used teletypewriter-based terminals the company had recently donated. A few years later, Creeper, the first modern computer virus was let loose on the ARPNET (a forerunner to the internet). It copied itself onto computers, leaving the short message: “I’m the creeper, catch me if you can!”

The term ‘virus’ was first used in a cybersecurity context in 1984, in a paper published by the University of Southern California. The modern concept of how cyber-attacks could affect society developed as the decade wore on. The first DEF CON hacking conference took place in 1993 and quickly became a popular annual cybersecurity event.

As the pace of digital advancement accelerated in the later 90s and into the new millennium, so did the chance for cyber-attacks and data breaches. Social media appeared, mobile devices became more common in the home and at work, and ecommerce exploded. Each development offered criminals new opportunities for exploitation, as well as the chance for well-meaning users to make costly mistakes.

In a little over a generation, the concept of cybersecurity has gone from a relatively obscure conversation to a mainstream international priority. Its implications have shifted from academic experimentation to a question of economic, civic and state security. Governments must now protect connected critical infrastructure 24 hours a day. Failing to shield vital services and resource networks effectively would quickly impact the lives of millions of people.

From an organizational standpoint, cybersecurity has long ceased to be the sole responsibility of the IT department. The right awareness and knowledge must inform and guide the daily activities of everyone in the workplace. Using internationally recognized standards in cybersecurity system design, and employee training, helps improve data protection and legislative compliance.

This report examines a number of key issues within cybersecurity, outlining how standards can be applied to boost organizational resilience. It ranges from protecting employees using personal devices for work tasks, to developing security standards for the burgeoning Internet of Things. It’s a useful starting point to discover which standards will optimize your organizational resilience.

John DiMaria
Global Product Champion for Information Security and Business Continuity at BSI Group

Contents

Bring Your Own Device (BYOD) arrangements and controls:

A standards-based approach

Increasingly popular, BYOD sees employees using personal devices such as laptops, tablets and smartphones for work activities, connecting to corporate networks and generating or storing data. A standards-based approach helps organizations mitigate security risks associated with BYOD arrangements.

According to a report by MarketsandMarkets, the BYOD and enterprise mobility market is estimated to grow to $73.3 billion by 2021[1]. However, BYOD still divides opinion – some see productivity gains and cost-saving potential, while others are more mindful of possible data breaches.

Having a specific BYOD policy, created in accordance with the ISO/IEC 27001 Information Security Management and ISO/IEC 38500:2015 (IT Governance) standards, should now be considered a minimum level of corporate protection.

Employee awareness and understanding of BYOD security responsibilities are critical to organizational risk. Regular communication of best practice in this area is important for people in all areas and at all levels of the organization. It's not enough to assume all staff will educate themselves to the required standard.

Consider how common it is to skip to the end of a terms and conditions form and just accept, without reading or engaging with the copy. Everybody must be invested in the process and given the chance to provide feedback and make suggestions. Individual responsibilities must be communicated to staff on a regular basis. The aspirational scenario is to have well-trained, proactive employees looking out for each other and the organization, providing coaching and interventions as required.

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

As well as getting new employees on board, a standards-based BYOD policy must include detail on procedures for when staff leave an organization. This is particularly important when employees are not leaving of their own free will. Organizations can request certain actions when an employee leaves, for example file deletion, but a BYOD policy should outline how this will occur.

It should also clarify whether the individual is trusted to carry out the actions themselves, or if the IT department must undertake them. It's important to follow the policy as quickly as possible once it's confirmed that an employee is leaving. There's a strong likelihood they'll use their mobile devices in their new workplace, in which case the difficulty in obtaining any required data is multiplied.

Legislative changes, such as the General Data Protection Regulation (GDPR), must also be considered when designing or updating a BYOD policy[2]. In strengthening personal data protection for EU residents and citizens, GDPR changes the way every organization collects, holds, processes and shares an individual's data.

Mobile device and BYOD policies must reflect GDPR requirements, particularly around subject access, data discoverability and data collection. The GDPR places responsibility firmly with the organization to produce the required data or files, rather than the individual.

The BS 10012 Personal Information Management System standard helps organizations demonstrate the required level of competence in GDPR-critical areas. The risk of data breaches from mobile devices can also be reduced by using well-maintained management applications to separate a user's personal and professional files, however BYOD policies based on established standards are the best protection possible.

Employee behaviour must also be accounted for outside the usual workplace. For example, when mobile device users are away from their usual working environment, their susceptibility to threats such as phishing tends to increase (employees are more likely to neglect security responsibilities if accessing non-work related content).

Wombat Security's 'Beyond the Phish 2017' report found that almost a quarter of people surveyed answered questions on protecting mobile devices and information incorrectly[3]. It also found that 14 per cent of UK workers have no locking mechanism on their mobile devices.

Finally, when mistakes are made, education is essential, whether delivered in person or through a specific software application. Having an up-to-date incident response plan clarifies immediate responsibilities and ensures the correct action is taken to contain and control the situation in the event of a breach. The emphasis must be on continuous risk assessment and testing to ensure security and BYOD policies remain effective ●

References

1. www.marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html
2. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
3. Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish

The Internet of Things:
Standards and security

Tim McGarr, Market Development Manager at BSI, explains why security is key to ensuring the Internet of Things market reaches its full potential.

Although the Internet of Things (IoT) offers significant improvements to our daily lives in terms of efficiency, automation and overall optimization, more work is needed to develop unilateral security standards to protect individuals, organizations and their data.

The IoT refers to any object connected to the internet which independently shares the data it collects over a network. From wearable fitness technology transmitting a user's heart rate and respiration to the cloud, to buses communicating with traffic control systems in cities, each data point gathered and measured contributes to an almost limitless opportunity to refine, control and optimize our daily lives.

The IoT market is projected to grow globally from USD 2.99 trillion in 2014 to USD 8.9 trillion in 2020, attaining a 19.92 per cent compound annual growth rate (CAGR)[1], and promises potentially transformative efficiencies and innovations. However, because the IoT is so wide-ranging and pervasive, the scope for cybersecurity breaches presents a major challenge. For example, an organization might have several of its systems connected to the internet to maximize efficiencies through data sharing and automation. Perhaps its heating, ventilation, air conditioning systems, machinery, building security and environmental sensors are all linked to the IoT and each other. This situation increases security complexity and risk, as well as the number of possible 'backdoors' or ways into a system for hackers.

In 2015, the Western Ukraine electrical grid was attacked, leaving almost 250,000 people without power for six hours. The attack overtook substation supervisory control and data acquisition (SCADA) systems and disabled their remote operation[2]. Another recent example was the widely-reported Mirai malware that exploited many vulnerable IoT devices during late 2016 in several different incidents, taking control of them to launch large-scale network attacks[3].

Beyond the digital realm, the safety implications for drivers of connected and autonomous vehicles (CAV) during a targeted cyber-attack on the controlling network, or even individual vehicles, make our physical vulnerabilities immediately clear.

The IoT market needs widely accepted best practices and standards in order to inspire greater public trust. Particularly important is the security of the data collected, shared and processed, as well as access to the devices themselves. Each month sees the launch of new IoT-ready objects. However, each manufacturer will vary in their approach to security. Without following the guidance in standards like ISO/IEC 27001, it's difficult to reassure the wider market that appropriate safeguards and controls were followed in the product design process.

With such a fast-growing emerging market, there are many more questions which must be asked for each new IoT-ready device, such as:

- What security certifications does the cloud infrastructure host hold?
- Has the manufacturer made efforts to educate prospective users around the importance of basic security awareness, such as changing default passwords?
- Which data encryption standards does it use? How about access control and user authentication?

BSI is taking a leadership role in this area, developing the PAS 212 'Automatic resource discovery for the Internet of Things' specification, in conjunction with the Hypercat Alliance.

Closely related to this are PAS 182 and 183. PAS 182 includes discussion of important security considerations central to implementing smart city concepts, including the interoperability of systems and data-sharing between agencies. PAS 183 defines a framework for data sharing between cities, setting out guidelines for appropriate usage and clarifying which types of data can be published and shared and what should be kept private.

Looking ahead, standards will remain central to how individuals and organizations prepare for, and mitigate, IoT security risks. The global nature of its growth demands a truly collaborative and international approach to security standards development and maintenance. BSI is committed to creating an inclusive community to tackle this challenge and accelerate IoT security standards adoption ●

"The IoT market needs widely accepted best practices and standards in order to inspire greater public trust."

The IoT market is projected to grow globally from $2.99 trillion in 2014 to $8.9 trillion in 2020

References

1. www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#9e2d8981480e
2. www.incapsula.com/blog/critical-infrastructure-cyber-security.html
3. www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

Cybersecurity trends and statistics

90%

of the data in the world today has been created in the last two years alone[1].

54%

of US workers believe they can trust open WiFi networks in trusted locations.[2]

More than half

of US and UK workers would leave a corporate laptop in their car rather than take it into a restaurant with them[3].

A Yobibyte =

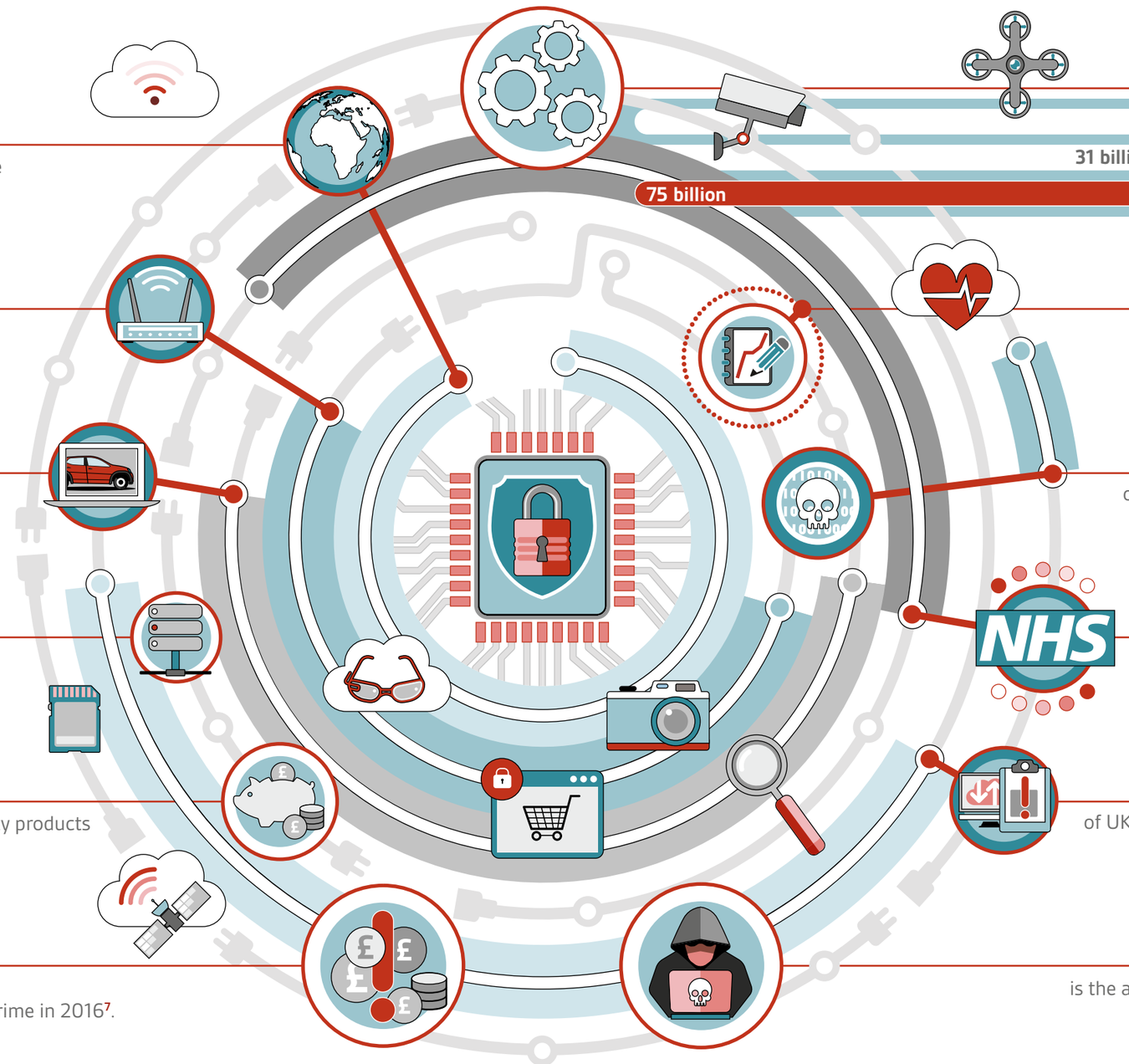
1,208,925,819,614,629,174,706,176 bytes[4].

$93 billion

Worldwide spending projected on information security products and services in 2018[5].

$6 trillion

Cybercrime damage costs to hit annually by 2021[6].
Globally, cybercrime was the second most reported crime in 2016[7].



Devices connected to the IoT[8]

Almost 60

data records are lost or stolen every second[9].

Only 4%

of recorded data breaches were 'secure breaches' where encryption was used and the stolen data was rendered useless[10].

42%

of NHS Trusts have not completed the UK government's '10 Steps to Cybersecurity' programme[11].

40%

of UK workers who installed a VPN said they rarely or never use it[12].

146 days

is the average time hackers stay hidden on a network[13].

References

1. www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/
2. 3. 12. Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish
4. https://techterms.com/definition/yobibyte
5. www.gartner.com/newsroom/id/3784965
6. www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
7. www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
8. www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
9. 10. https://breachlevelindex.com/
11. www.information-age.com/uks-critical-infrastructure-skipping-basic-cyber-security-checks-123468204/
13. www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

Cybersecurity and protecting critical infrastructure

John DiMaria, Global Product Champion for Information Security and Business Continuity at BSI Group, describes how a standards-based approach is the most effective way of mitigating internal and external threats.

Governments generally define the essential assets of a functioning society as its critical infrastructure, for example electricity, communications, heating, healthcare and transport networks. The consequences of one or more of these major systems becoming unavailable, even for a short time, would immediately impact the lives of millions of people.

Modern national infrastructure networks are increasingly interconnected and interdependent – sharing data and information to drive increased efficiency and control. However, this increases the vulnerability of the entire system, whereby a single asset failing will have a cascading effect across the wider connected network. Ongoing risk assessment and mitigation is therefore vital for their protection, especially from a cybersecurity perspective.

Critical infrastructure will always be the subject of attempted cyber-attacks. Aside from their vital importance, hackers are attracted to the multiple opportunities they present for infiltration. For example, a global infrastructure survey, carried out in 2017, saw 67 per cent of respondents report multi-vector distributed denial of service (DDoS) attacks, up from 56 per cent in 2016. These attacks combine volumetric, application-level and protocol-level elements, making them much harder to defend against[1].

Many large infrastructure networks are also not adequately protected. A 2017 survey of 338 critical infrastructure organizations in the UK showed that 42 per cent of NHS Trusts had not completed the UK government's '10 Steps to Cybersecurity' programme, first issued in 2012. Also, more than half of these organizations were judged to be ignoring the risk of swift and stealthy DDoS attacks on their networks - commonly used to plant malware, ransomware and for data theft[2].

Furthermore, critical infrastructure networks in many countries are run by a variety of different private organizations, all working closely with government at local, regional and national levels. With so many groups and stakeholders involved, a harmonized approach to their cybersecurity is essential, using agreed best practices as a foundation.

BSI regularly convenes meetings, committees and working groups that bring together governments and companies responsible for critical infrastructure, to develop and maintain international best practices in a harmonious manner. This is how the ISO/IEC 27000 family of standards was developed.

Using established standards to create resilient protection for critical infrastructures demonstrates cybersecurity commitment to the wider market. It also delivers reassurance that the appropriate controls are in place. In addition, certification to recognized security standards is required for companies involved in most critical infrastructure supply chains. It allows prospective supply chain partners to transparently share and communicate their security credentials, and provides a framework for continual improvement, quality control audits and validation processes.

As well as mitigating against external cyber-attacks, a standards-based approach to protecting critical infrastructure will also reduce risks associated with human error. Specialist training, and performance assessment measures, help organizations develop security awareness across key staff groups to maintain standard of care responsibilities. Also, in the event of an incident investigation, being able to prove that organizational policies adhere to recognized international standards is often decisive in dispelling negligence claims.

Finally, it's worth noting that governments and legislators can't realistically be expected to keep pace with attacks from resourceful hackers in isolation, but long-term international collaboration to develop and maintain standards remains the most effective way to protect critical infrastructure and data on a global scale ●

“Using established standards to create resilient protection for critical infrastructures demonstrates a commitment to cybersecurity to the wider market.”

Further reading

www.ucl.ac.uk/rdr/cascading/resources/reports-guidelines/Report_Power_Failures

References

1. www.darkreading.com/cloud/7-things-to-know-about-todays-ddos-attacks/d/d-id/1329758?piddl_msgid=329347&image_number=3
2. www.scmagazineuk.com/critical-infrastructure-not-ready-for-ddos-attacks-foi-data-report/article/684838/

Data privacy, compliance and GDPR

John DiMaria, Global Product Champion for Information Security and Business Continuity at BSI Group, describes how standards-based data governance is the best route to regulatory compliance.

In 2018, the General Data Protection Regulation (GDPR) superseded the data protection directive of 1995, which was no longer able to protect personal data relevant in an age of internet and cloud giants like Google and Facebook.

The pace of legislation rarely matches the speed of technological development and the social and commercial transformation it drives. The GDPR is a particularly good example of legislation slowly catching up with technology. In the years between the GDPR's inception (2011) and enforcement (2018), we've seen the smartphone explosion, voice search and the Internet of Things (IoT) become mainstream. However, the fundamentals of good data governance have remained reassuringly consistent, even if the complexity of the threat and the opportunities for data breaches seem to have multiplied.

The GDPR introduces tougher penalties and fines for non-compliance, and unequivocally places responsibility with the organization, giving EU residents and citizens ultimate control over their personal information. It's the most significant update to existing European data privacy laws in half a generation, with much discussion in the mainstream media during the run up to its May 2018 implementation deadline.

Despite this, it's important to remember there are over 100 other different territorial data privacy regulations – each with varying requirements and stipulations. A standards-based approach to organizational data governance is the best foundation for working towards consistent global compliance.

Using recognized standards to inform data protection processes helps companies understand their current, and potential, levels of exposure and provides a framework of controls to manage or reduce them. Certification helps to gain stakeholder and customer trust, and reassure both that their personal data is protected. In fact, many forward-thinking businesses saw the approach of GDPR as a distinct reputation-building opportunity.

BS 10012 provides a pathway for companies to define their GDPR risks and compliance requirements, then implement a personal information management system in a way that's best for their business. Once the system is in place, organizations can request independent certification to demonstrate their effective management of personal data and ensure that their processes are maintained to deliver continuous improvement.

Finally, certification to recognized data governance standards also increases transparency between supply partners, reassuring all parties that appropriate controls are in place and pushing accountability far down the chain ●

The five W's of data and other relevant standards

BS 10012 helps companies manage the five Ws of data, namely:

1. Whose data is it?
2. Why are we processing it?
3. Where is it kept or transferred to?
4. When are we keeping it until?
5. What safeguarding mechanisms do we have in place?

Other relevant standards include ISO/IEC 27018 to help protect personally identifiable information in the public cloud, ISO/IEC 29151:2017 for a set of additional controls aligned with ISO/IEC 27001, BS ISO/IEC 38505-1:2017 for data governance and controls over the flow of information and a new emerging standard: ISO/IEC 27552 extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management - requirements and guidelines.

10 key cybersecurity standards

ISO/IEC 27001	Information security management.
BS EN ISO/IEC 27002:2017	Reference handbook for selecting controls within an information management system.
BS ISO/IEC 27003:2010	Information security management system implementation guidance.
BS ISO/IEC 27005:2011	Information security risk management.
ISO/IEC 27017	Security controls for cloud services.
ISO/IEC 27018	Protecting personally identifiable information in the public cloud.
BS ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity.
BS ISO/IEC 27032:2012	Guidelines for cybersecurity.
BS ISO/IEC 27033-1:2015	Network security overview and concepts.
BS ISO/IEC 27034-5:2017	Protocols and application security controls data structure.

What is GDPR?

The General Data Protection Regulation (GDPR) from the European Parliament, the Council of the European Union and the European Commission represents a long-awaited strengthening of data protection.

It allows citizens and residents of the European Union (EU) to take control of their personal data, replacing the data protection directive of 1995, which was created before the internet became mainstream. The regulation is also intended to improve public trust in the burgeoning digital economy, considering the way modern giants like Facebook and Google gather and use individuals' data.

Although the GDPR introduced tougher penalties and fines for non-compliance and breaches, it provides businesses with more legal clarity and unifies data protection law across the single market[1].

GDPR introduces several important requirements, including changes to:

- Consent, which must be actively affirmed by the data subject and recorded by the data controller
- What counts as personal data
- Requests by individuals for information on how personal data is held and used, timeframes for response by organizations, and requests for data to be deleted
- Timeframes and protocol in the result of a data breach

Data controller vs data processor

The GDPR defines two key roles in an organization – the data controller and the data processor.

The controller refers to the person or people who determine why and how the personal data will be processed. The processor is the person or group(s) carrying out the processing work on the controller's behalf.

Both the controller and processor must now demonstrate GDPR compliance.

Reference

1. www.eugdpr.org

CONTROLLING VULNERABILITY

"...the fundamentals of good data governance have remained reassuringly consistent, even if the complexity of the threat and the opportunities for data breaches seem to have multiplied."

Mitigating the risk from human error

David Maher, International Marketing Director, BSI Cybersecurity and Information Resilience, outlines the challenges that companies face in today's cloud-based landscape.

Human error will always be part of an organization's cybersecurity risk profile, and is often seen only as a possible weakness. However, standards-based training has the potential to transform it into an area of strength.

People are often described as the weakest cybersecurity link, given that human error is responsible for a high percentage of security and data breaches each year. With this in mind, the importance of standards-based awareness training, and education, cannot be overstated.

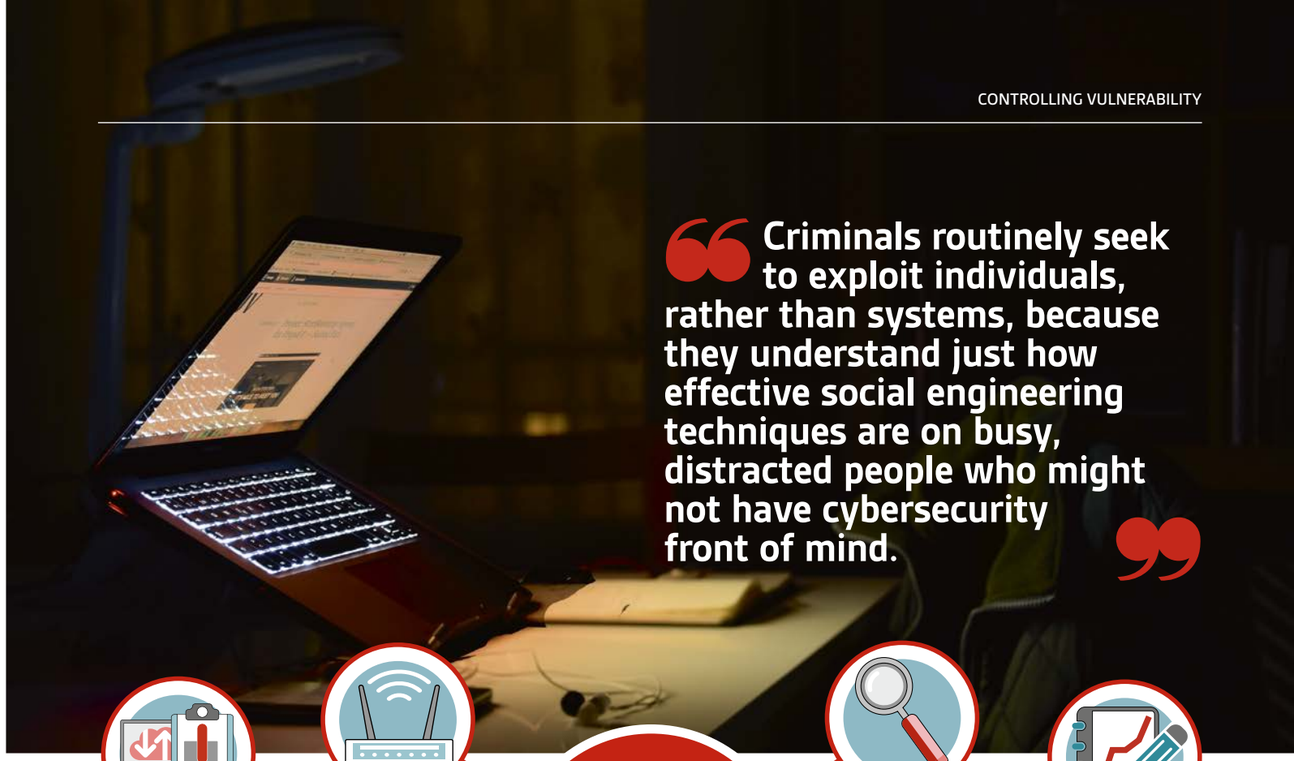
Criminals routinely seek to exploit individuals, rather than systems, because they understand just how effective social engineering techniques are on busy, distracted people who might not have cybersecurity front of mind. Wombat Security's 'Beyond the Phish 2017' report revealed that almost a quarter (24 per cent) of respondents answered questions relating to identifying phishing threats incorrectly. This highlights the significant opportunity for those looking to steal data and identities by manipulating a lack of awareness[1].

Rather than take a reactive mind-set, companies should work to make their employees a stronger link in the cybersecurity chain – empowering them to become a 'human firewall'. This is particularly important given the rise of home working and the popularity of employees using personal devices for work. Cybersecurity awareness must extend beyond an employee's regular workspace.

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.

Wombat Security's research found that the average employee also lacks awareness when it comes to supposedly simple safeguards. For example, over half of US workers believe they can trust open WiFi networks in trusted locations, 40 per cent of UK workers who installed a VPN said they rarely or never use it and more than half of US and UK workers would leave a corporate laptop in their car rather than take it into a restaurant with them. The study also highlighted common training needs around physical security, such as protecting items like ID badges, printed information and files that provide details about suppliers[1].

Consideration should also be given to how cybersecurity training content will be delivered. Taking an annual approach to training will not provide the desired results, or engage staff. We recommend short, but frequent, training, as well as targeting employees with consistent content. To make a real change in behaviour, it's also important to create a culture of involvement, as giving staff the chance to provide feedback and make suggestions increases their engagement.



> **Criminals routinely seek to exploit individuals, rather than systems, because they understand just how effective social engineering techniques are on busy, distracted people who might not have cybersecurity front of mind.**

91 per cent

of cyber-attacks start with a phishing email[2]

Standards-based cybersecurity training can help foster genuine awareness amongst employees and embed individual and collective responsibilities within staff at all levels. With improved understanding of the risks, employees are much more likely to report anything suspicious, becoming a highly effective first line of defence.

It's also important to introduce quick and easy reporting mechanisms for anything suspicious. Even with an optimal cybersecurity system in place, errors will still occur, although their significance and severity should be significantly reduced.

Maintaining an up-to-date incident response plan will clarify immediate responsibilities and ensure correct action is taken to contain and control the situation. Event details should be recorded to guide ongoing learnings and continuous risk assessment. Specific post-event training and education may also be necessary.

Finally, proving that an organization is certified to (or uses and follows) recognized standards in its cybersecurity training and processes is important. In the event of any data breach, it helps demonstrate that a company has the necessary controls in place to reasonably and responsibly fulfill its duty of care ●

References

1. Beyond the Phish Report 2017, published by Wombat Security: www.wombatsecurity.com/beyond-the-phish
2. PhishMe, 2016: www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

Online access to cybersecurity standards: BSOL

75 per cent
of businesses said ISO 27001 reduces business risk[1]

Cybercrime costs the global economy hundreds of billions of dollars per year. BSI has the essential standards you need to protect your business, employees and customers. BSOL is our online standards library, guaranteeing instant access to the right cybersecurity standards.

Using out of date information to protect critical systems and data could have serious consequences. Available 24 hours a day, BSOL allows subscribers to view and download the latest cybersecurity standards, as well create specific alerts and email notifications around updates.

Essential cybersecurity standards to get you started

ISO 27001:	Information Security Management Systems. This is the foundation of every effective cybersecurity strategy.
ISO 27002:	Information technology. Security techniques. Code of practice for information security controls.
ISO 27003:	Information technology. Security techniques. Information security management systems guidance
ISO 27005:	Information technology. Security techniques. Information security risk management.
ISO 27017:	Information technology. Security techniques. Code of practice for information security controls based on ISO 27002 for cloud services.
ISO 27018:	Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
ISO 20000-1:	Information technology. Service management.

To request a demo or to find out more please call +44 (0)345 086 9001 or email cservices@bsigroup.com

Reference

1. The Economic Contribution of Standards to the UK Economy Report, published June 2015 by Cebr & BSI.

Disclaimer

Cybersecurity: Training and certification with BSI

Getting staff trained on key cyber-resilience and security standards, such as ISO/IEC 27001, is central to how leading organizations approach cybersecurity. BSI provides training courses to suit every cybersecurity need, as well as those specifically designed for senior leadership.

After standards have been successfully introduced, getting independently certified sends a message that your organization is committed to excellence in information security.

1 Get involved with standards

Using recognized standards in cybersecurity planning and processes allows organizations to fine-tune compliance and mitigate against day-to-day risks. Standards promote efficient and sustainable operations, demonstrating the quality of your processes to customers and partners.

2 Get standards training

Whether you are new to using standards or need advice on maintaining or auditing an existing certification, BSI has a range of training courses to suit your needs, as well as those specifically designed for senior leadership. BSI courses include GDPR, information security compliance, eDiscovery, digital forensics training and end-user awareness.

3 Get standards certification

BSI certification demonstrates to your customers, competitors, suppliers, staff and investors you have addressed and mitigated cybersecurity risks, and will continue to do so. This is important for every organization, large or small. Also, BSI experts don't just assess your compliance to standards, they support you every step of the way so you can continually improve.

4 Get cybersecurity help*

Our professional services teams help organizations prepare for specific events, as well as handle unforeseen situations. BSI provides penetration testing services to address weaknesses in your network before they are exploited as well as insights and solutions for a range of data protection issues. Our incident response services help you take action in the event of a breach or ransomware attack.

bsi.

*If you purchase cybersecurity help in the form of consultancy services, you will have to engage a certified body other than BSI for any information security management system certification, to ensure there is no conflict of interest.

bsi.

...making excellence a habit.™

If you would like to find out more about creating your own digital standards collection via BSOL, please get in touch:

389 Chiswick High Road,
London W4 4AL UK
Tel: +44 345 086 9001
E: cservices@bsigroup.com
www.bsigroup.com

23rd Floor, Cambridge House
TaiKoo Place
979 Kings Road
Island East
Hong Kong
T: +852 3149 3300
E: BSOLAPAC@bsigroup.com

12950 Worldgate Drive
Suite 800
Herndon
VA 20170
T: +1 703 608 5693
E: Karen.jacobs@bsigroup.com