The Challenges Facing CISOs Today

Strengthening resilience in a digital world

A whitepaper

bsi.

...making excellence a habit.™

Introduction

Chief Information Security Officers (CISOs) have a multitude of challenges that need to be met head on. Traditional information management challenges have broadened to accommodate the growth in technology channels, data size and an ever-evolving cybersecurity landscape.

CISOs need to apply risk management techniques to meet business strategy and objectives while ensuring security measures are applied in an appropriate way. Building your organization's security posture via an incremental, always-improving model yields long term security maturity. This should always be the goal.

In this paper, we will walk through some of the most common challenges that CISOs face, from cloud migration through staffing, data management, culture and automation outlining the best approaches that you can take to tackle these issues.

Call: **+44 345 222 1711 /+353 1 210 1711** Email: **cyber@bsigroup.com** Visit: **bsigroup.com**

Culture

Underpinning all the challenges facing the CISOs is the requirement to create a culture of security awareness within the organization. The more people understand it, the better equipped your organization will be.

There may be legacy culture and out-dated mindsets that require 'modification' – this is a people engagement. Outlining the risks and benefits to the organization can help sway perceptions. A security communication plan detailing the schedule, forms of communication and contents to be communicated should be drawn up and executed on a regular basis.

Security is an iterative process that builds up over time, starting by getting the fundamentals right. Continuous communication, security awareness training and simulated security exercises will ensure the message is received and understood by employees.

Measuring current state

Understanding an organization's current state, which of course is changing on a daily basis, is imperative.

CISOs can arm themselves with the knowledge of where to prioritize efforts for future state requirements by measuring current security profile, completing gap analysis exercises and monitoring and analysing measurement trends. The establishment and development of security metrics such as Key Risk Indicators (KRIs), creation of balanced scorecards for executive management and communication of this information to team members, also help drive awareness of the security progression.

Organizational Structure

Understanding the internal organizational structure of the company is also important. To whom does the CISO report? Currently, reporting lines for CISOs tend to be split between the CEO, the CIO and other C-level executives.

The reporting line needs to be determined according to the business strategy and it must also be appropriate for the organization. Even though, some regulators have begun to mandate that CISOs should report to the CEO. A recent study has found that, in Israel for example, there are laws dictating that CISOs report directly to the CEO.

The autonomy of CISOs to fulfil their role of protecting the organization is crucial and needs to be fully understood at a board level.

Stakeholder Management

Stakeholder engagement is particularly important for CISOs. Keeping board members regularly updated about information, security related business risks, active budget engagement and realization of benefits is all crucial to getting widespread buy-in.

Employees need to be informed of all aspects of the security programme that relates to them. They must also know and understand the risks associated with not understanding the fundamentals of safe cybersecurity behaviours.

For organizations that are subject to regulations, a working relationship with the regulatory authority can be beneficial both in terms of being proactive with regulatory requirements and with reactive incident management engagement.

As the role of CISO spans the width of the organization, the integration of security requires broad buy-in from the other IT functions. Engaging with the technical team leaders such as the network, database, server and storage teams, ascertaining their security, data protection and business continuity levels and implementing a continuous security improvement programme, will all result in a more mature security capability.

Industry Developments

Keeping abreast of the rapidly changing environment is a workload. In order to make informed decisions, CISOs must be aware of all relevant developments in the industry.

Building experience and knowledge in your security team can be enhanced by:

- subscribing to blogs, podcasts and webinars
- attending seminars and industry events
- developing personal development plans
- using collaboration technologies to share information and links of interest
- utilizing the expertise of a security advisor or outsourced expert body

National bodies such as the National Institute of Standards and Technology (NIST) in the US, the National Cyber Security Centre (NCSC) in the UK and the European Network and Information Security Agency (ENISA) in the EU all provide valuable information security guidance.

Supply Chain

As organizations grow and adapt new technologies, their supply chains become longer and more complex. Dependencies build up over time and ongoing security assessments of suppliers are essential.

A comprehensive onboarding process, review of technology controls and attestations, protective legal and service level agreements that meet business requirements are essential to mitigate supply chain risks and manage issues if they arise.

Cloud Technologies

The rate of growth of the cloud technology stack over which CISOs must maintain a controlled security posture is quite staggering.

With the DevOps culture currently in place, Cloud Service Provider (CSP) are constantly manipulating their SaaS software code to reflect new features, user interface (UI) improvements and bug fixes and client feature requests. From a CISO perspective, security controls, pen-test results and remediation/audit reports are thus only valid for an ever-smaller timeframe.

The integration of on-premise, data center and cloud-based data sets and applications add further complications that demand assessment and action. Therefore, CISOs and their teams need to:

- review release notes from the CSPs
- subscribe to CSP technical blogs
- register for CSP webinars as they outline new and imminent developments
- engage with CSP account managers through a formal process (e.g. quarterly business review)

Aligning with business and application owners helps the CISO to construct an informed view. In conjunction with the extensive use of SaaS and the more involved use of PaaS and IaaS (due to the flexibility, speed to market, cost modelling and feature rich functionally offered by CSPs), CISOs need to be aware of both these functions and also their organization's use or intended use of the platforms.

Engagement with the project management office (PMO) and development teams, communicating the organization's risk tolerance and risk management practices and deploying appropriate technology will help CISO to maintain appropriate governance, risk and compliance (GRC) stance on the use of cloud services.

Vulnerability and Configuration Management

Operating Systems (OS) remains a concern for CISOs, with the cessation of security support for legacy Windows OS such as Windows 7 and Windows 2008 (R2) server editions and the ongoing bi-annual release of Windows 10 updates.

When we factor in the mobile and server OS requirements, challenges include the broad range of OS versions, varying levels of vendor support, diverse patch deployment methods and reporting. In conjunction with OS management, CISOs must also consider the risks associated with devices management (e.g. shadow IT).

While a standardization programme will help with some of these challenges, it may not always be possible in a global organization where the use of diverse technologies in conjunction with the extraction and consolidation of data, may be required to fulfil reporting and risk requirements.

Automation

There has been much discussion around automation in security. The scarcity of staff, combined with the volume of data, leads to the use of automated tools to streamline those low-value and high-volume events.

Security orchestration, automation and response (SOAR) brings together the collective of security technologies employed by an organization. By analysing threats, prioritizing them from a business perspective and implementing automatic remediation processes, these changes can balance the security team's workload, freeing them up for more advanced threats that are outside the SOAR scope.

While several technology companies offer automated security response platforms, CISOs must be analytical in their approach to these tools and decide – based on individual requirements – how far up the technology stack the tools may be allowed to operate. Balancing the ceding of control while maintaining accountability is key.

Data Management

The management, security and operational use of data have never been more important.

The value of data can be based on both the explicit use for which it is provided and, in many cases, by its implicit use when it comes to metadata. CISOs must have a strong understanding of the data lifecycle. They must also work closely with data owners to ensure information is secured throughout its journey within the organization.

A data mapping exercise can determine data location, size, ownership and age. This allows CISOs, in conjunction with other parties, to ascertain which data requires action under data retention and destruction policies. Aside from the security and privacy requirements, this exercise helps organizations to control costs in the hosting and backing up of data, as well as eliminating the responsibility to produce aged data if an electronic discovery and freedom of information request or similar GDPR order is made.

It's worth noting that CISOs must not restrict themselves to only the electronic versions of data but should also work with stakeholders on physical copies which are subject to the same policies and lifecycle.

Incident Management

As organizations grow, their attack 'surface areas' increase and they become ever more attractive to criminals. Against this backdrop, security incidents are inevitable.

Malicious breaches, ransomware, email attack vectors, state-sponsored cyber activity, Advanced Persistent Threats (APT), intellectual property theft and insider malpractice (deliberate or accidental) have all made headlines in the last year. When these incidents do take place, the spotlight falls firmly on the CISO and the Incident Management (IM) process they have in place.

Following a standardized or customized IM model (i.e. to reflect an organization's culture or strategy) can help to offset what can be an extremely damaging situation.
The cost of incidents can only be calculated several months later as reputational damage, share price, loss of business, staff turnover, regulatory fines and the cost of clean-up are calculated.

With GDPR having taken effect, regulatory incidents are coming ever more to the fore. Knowledge of all regulations, particularly when it comes to know where data resides globally and a good working relationship with the organization's compliance and legal teams, are essential to meet Governance, Risk and Compliance (GRC) requirements.

Identity Management

As data and applications move beyond an organization's assets and users' working models become more flexible, the use of Identity and Privileged Access Management (IAM\PAM) has advanced hugely in recent times, with extended reach into cloud services.

Organizations are increasingly moving towards a zero trust-based identity model by using:

- Federated identities
- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- Application management
- Geo-locational awareness
- Role-Based Access Controls (RBAC)
- Principle Of Least Privilege (POLP)
- One-time / time-limited / system restricted passwords

Securing user identities is a crucial business decision and CISOs should advise executive management on the trade-off between the use of public CSP offerings and third-party identity providers.

Social Media

Social media activity is of course extremely prevalent in today's business world, helping large and small organizations to promote their activity. CISOs need to be aware of all social channels being used by the organization and take all security measures to secure those channels.

Engaging with departments such as Marketing to assist with controls such as MFA, helps to minimize the risk that corporate accounts are compromised. Employees should also refrain from providing too many details (e.g. like confidential information or company identifiable details) via LinkedIn or other accounts to hamper social engineering attempts. Similarly, out-of-office messages should be customized between those sent internally and those sent externally.

Some providers offer technologies that assist the governance of social media activity, placing themselves inline between users and social media platforms to enable organizations to monitor and protect themselves from negative or inadvertent communications.

Conclusion

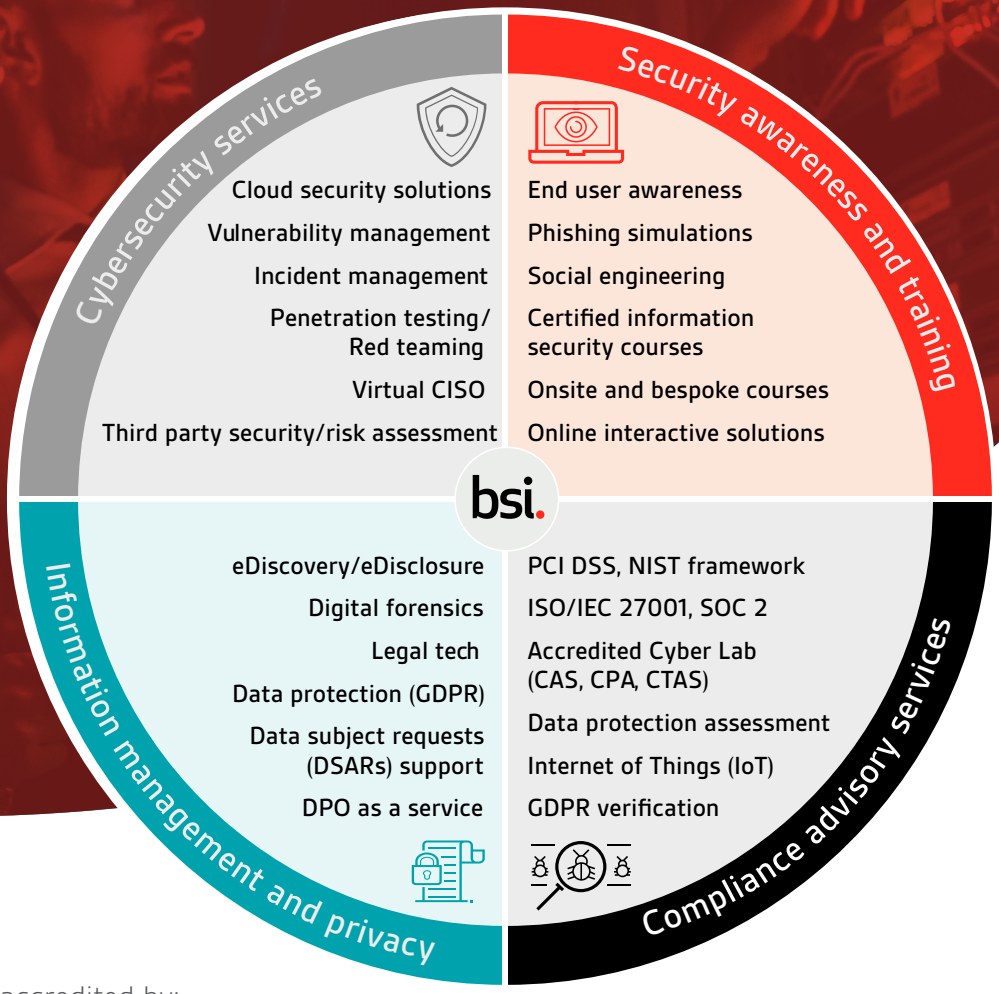
Today's CISO must bring a hybrid set of skills to the role. They must be pragmatic, business aware, people-orientated and technically minded. They must balance the requirements of the business against the constantly shifting security landscape and across multiple channels.

This can only be achieved by working with the business, understanding the organization's strategy, engaging with people at all levels, employing appropriate technology and ultimately building a team that is dedicated to ensuring the company remains security resilient.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Our expertise is accredited by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™ · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

Find out more

bsi.

UK	IE/International
Call: +44 345 222 1711	+353 1 210 1711
Email: cyber@bsigroup.com	cyber.ie@bsigroup.com
Visit: bsigroup.com	bsigroup.com