BSS.

How CISOs can succeed in a challenging landscape.

Reimagining operational resilience and recovery in 2023

www.bss.uk.com

Introduction.

Chief Information Security Officers (CISOs) are under increasing pressure to deliver information security strategies that defend their organisations from a continuously changing threat landscape. A robust information security posture is non-negotiable.

But information security and risk needs are complex and unique to every organisation. Business-wide priorities and solutions are not always clear, results are needed quickly, and everything needs to be on budget.

It's high time for upfront, realistic conversations about business objectives and the necessary tailored information security solutions and services that are vital to deliver results.

This report draws on new research from 150 information security leaders and sets out their top priorities and challenges, as well as insights into budgets and C-Suite buy-in. BSS want to show the need for investment and how the CISO can succeed in 2023 and beyond – cementing their role as a voice in the boardroom.

Mark Ampleford,
Managing Director at BSS

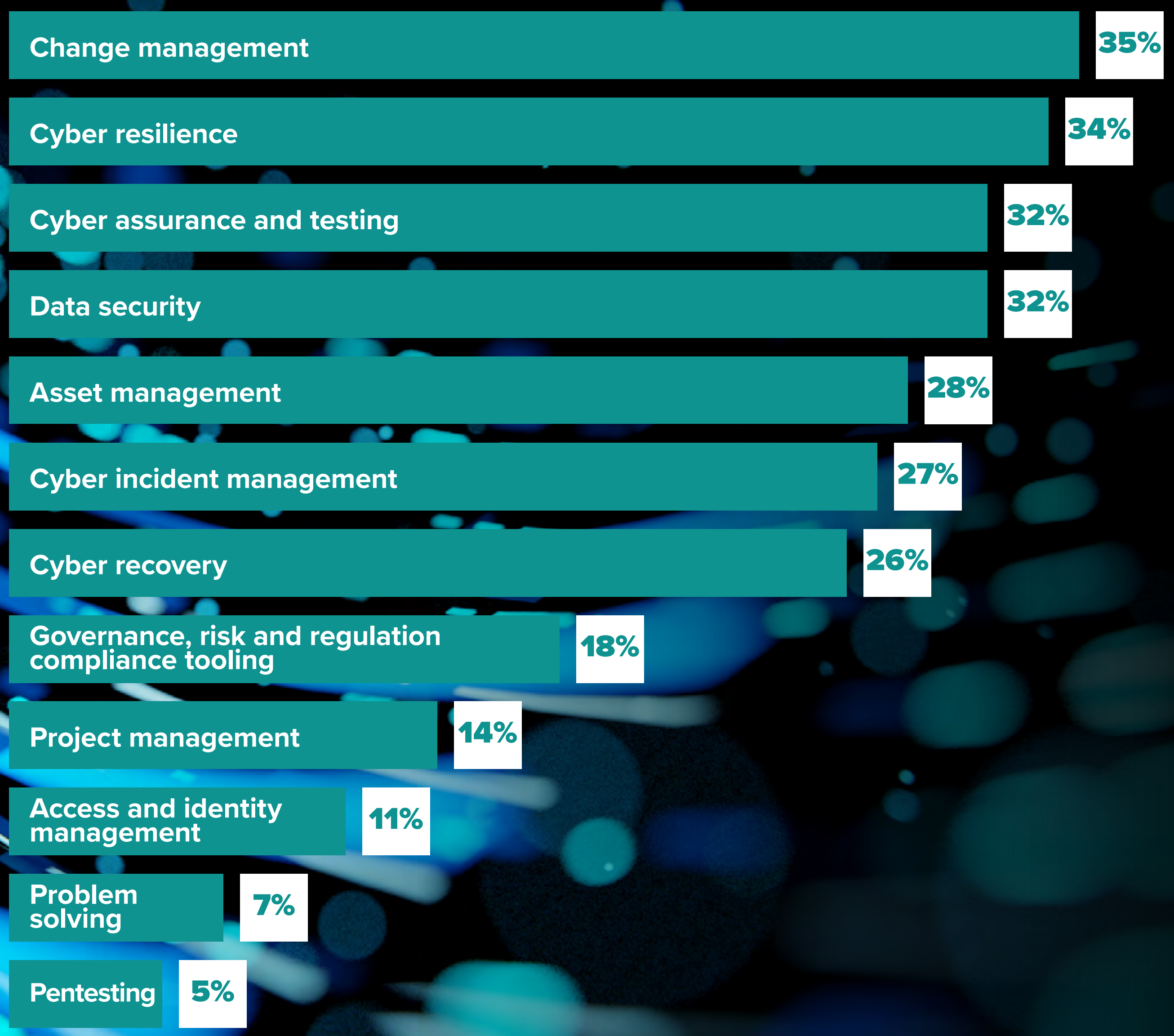
Research methodology
The research was commissioned by BSS and conducted online by global market research firm 3Gem in March 2023. The survey was conducted among 150 SecOps decision makers with titles such as Chief Information Security Officer (CISO), Chief Security Officer (CSO) and Technical Information Security Officer (TISO). All figures quoted come from this research unless stated otherwise.

Top CISO priorities.

Change, change, and more change. An organisation's information security, risk, assurance, and compliance needs never stop. But the right investment priorities can make a big difference in easing the pressure CISOs are under in the face of the evolving information security threat landscape.

The CISOs we surveyed said their top four highest investment priorities in 2023 are change management (35%), information security resilience (34%), data security (32%), and information security assurance and testing (32%). These findings suggest a certain amount of information security maturity from organisations of all sizes, but the basics should never be underestimated, and multiple challenges are scuppering progress.

CISOs highest investment priorities for 2023



Top CISO challenges.

Achieving confidence in security features, practices, procedures, and architecture is not simple, especially when internal teams are already stretched.

While every organisation must overcome complex security and risk challenges, there are some clear common challenges that our research has discovered.

1 Budgets don't match expectations.

It's positive to learn that 61% of respondents said their information security budget increased, and this wasn't just organisations with millions of pounds to spend. The highest finding was among CISOs with an annual security budget of £500,000 to one million pounds, with almost three-quarters (73%) saying they received a budget increase.

It is encouraging to observe that a majority of CISOs are experiencing a notable increase in funding, averaging between 10% and 30% more. However, this positive development can be accompanied by impractical expectations.

Over three-quarters (78%) of CISOs said high-profile incidents have changed attitudes to information security in their organisation, resulting in more budget. But when budgets do get increased, it's often for the wrong reasons.

Over half (55%) of those surveyed say they are expected to spend their budget on cyber security issues that are hitting the news headlines, rather than where it's really needed. This is problematic, given that prevention, not reaction, is the key to effective information security management.

2 Change management.

It is critical that CISOs keep pace with the degree of technological innovation alongside the evolving threat landscape. When executed effectively, change management helps organisations to plan and develop their security architectures and processes, enabling them to respond effectively to information security attack attempts.

From cloud transformation design, through to multi-person international change programmes in information security resilience and recovery, a structured process for evaluating a proposed system or service change is crucial.

With change projects requiring such a high level of organisation, it's no wonder that over a third of CISOs (37%) find it challenging to manage these projects. This pain increased further for CISOs of organisations with 500+ employees with over half (51%) reporting difficulty in managing change projects.

But, with the correct frameworks in place, the trap of assuming the information security team will just cope with every change project can be avoided. In short, it should not be assumed that existing security resources can consume the additional effort required to support all necessary changes.

3 Relentless regulations.

Keeping pace with relentless regulation changes is tough. For example, the UK government recently strengthened its Network and Information Systems (NIS) regulations, under which organisations failing to enact effective information security processes could be fined up to £17 million for non-compliance.

Meanwhile, industry bodies such as the Financial Conduct Authority (FCA) have set a deadline of March 2025 for financial organisations to have a robust information security plan for a satisfactory level of customer service in the event of a security breach.

It's no wonder that nearly two thirds (64%) of respondents told us regulations change before they can make good on previous requirements, with over a third (33%) of CISOs saying keeping pace with changing regulations has presented a significant challenge. Poor data governance only adds to this problem for another quarter of CISOs.

CISOs need to use the fact that financial penalties and brand reputation are on the line to give them leverage in the boardroom to get the resources and investment they need.

4 Supply chain security.

A quarter of CISOs (25%) report managing complex third-party supply chains as a top challenge. This increased to over a third (35%) of CISOs with £1m to £9m and £10m to £49m annual information security budgets – highlighting it's not all about budget but instead the focus needs to be on getting a framework to measure, manage, and assure supply chain risk.

The growing issue of third-party supply chains is recognised by the National Cyber Security Centre (NCSC) and they have issued a 12 step guide to establishing effective supply chain control.

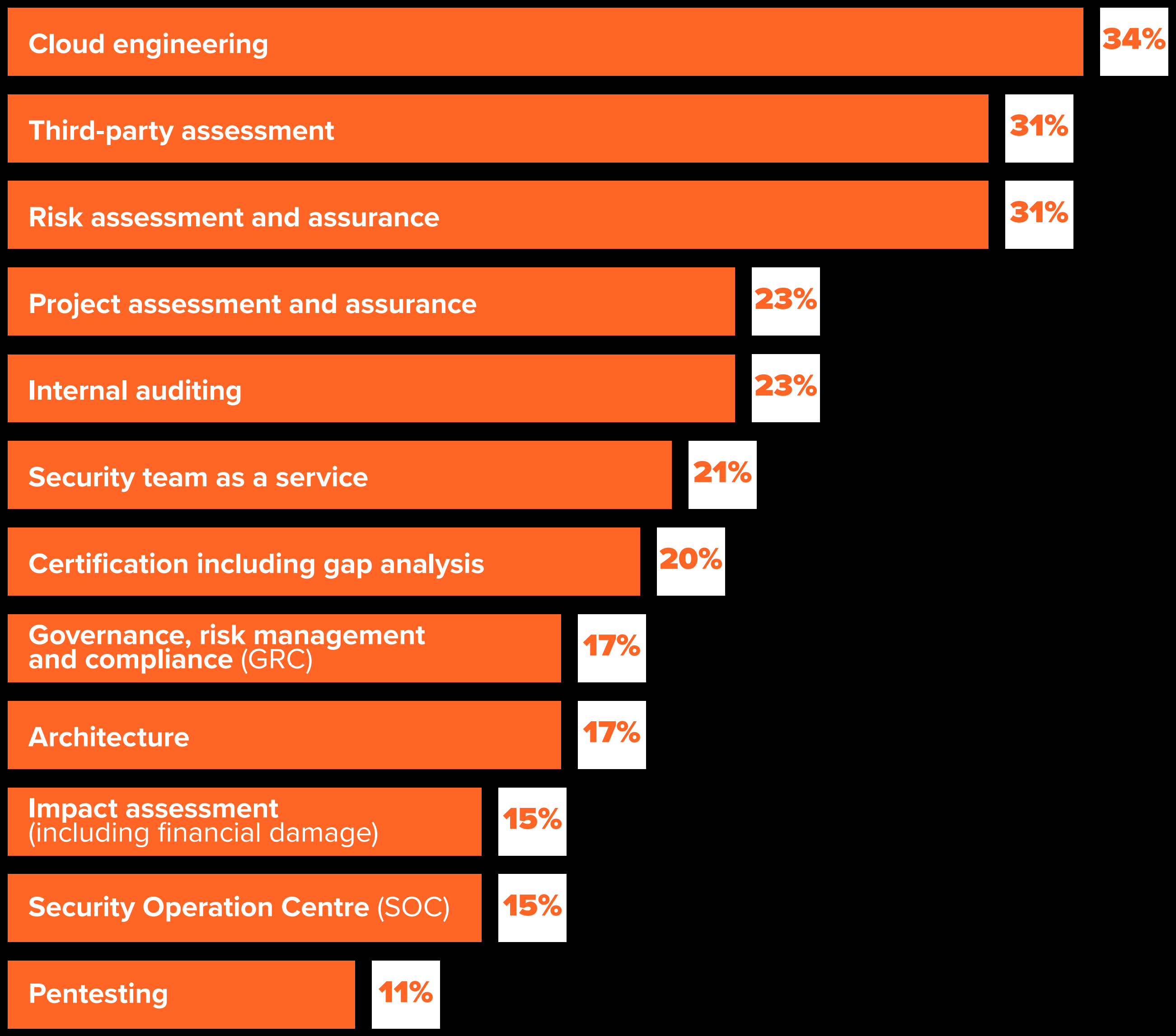
Any implementation and changes to third parties and wider supply chain risks must be regularly assessed, understood, and assured. Over a quarter of respondents (27%) admit they are locked into long-term and/or expensive supplier contracts. This is no excuse for a lack of understanding of the information security risks suppliers pose and ensuring they are kept accountable to meet your organisation's requirements.

Talent constraints.

The Department for Digital, Culture Media & Sport found half of all information security firms have experienced technical skills gaps, either among existing staff or among job applicants in its 2022 study. This ongoing skills shortage is a barrier for many CISOs to secure a permanent headcount for their information security teams and deserves its own section.

Nearly half (48%) agree their organisation suffers from a skills shortage. Most notably, our research identified a significant lack of expertise within cloud engineering, third-party assessment, and risk assessment and assurance, as well as shortfalls in a range of other disciplines. These gaps marry with the biggest challenges and priorities we've identified.

In which of the following areas of information security do you find it challenging to recruit and retain staff?

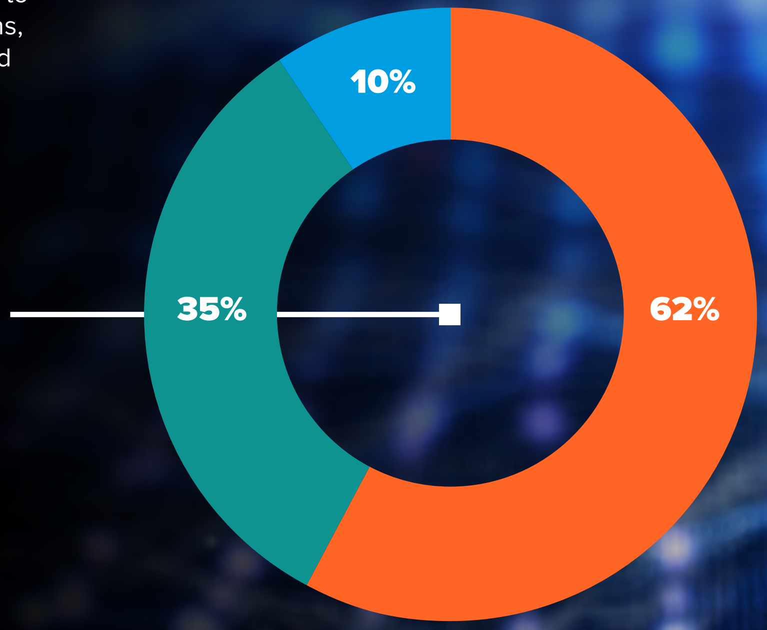


Interestingly, while the majority of our respondents reported a permanent headcount within their information security / SecOps teams, nearly two thirds (62%) stated that at least a quarter of their security specialism isn't based in the UK. And while hiring offshore personnel is a good way to boost resource, local knowledge of regulations, compliance, and risk, are benefits of UK-based experts that shouldn't be overlooked.

What percentage of your information security / SecOps team is based outside of the UK?

Key:

- 🟧 **Over a quarter**
- 🟩 **Over half**
- 🟦 **Over three quarters**



Job satisfaction and retention among CISOs is in flux too. Although recent research found the average tenure of a CISO is six years, at the same time over one in ten (13%) only stay in the role for less than a year. Such short tenures can lead to organisations falling behind, with high churn rates potentially causing information security strategies to falter and budgets to be misspent without experienced leaders at the helm.

Feeling valued by the wider business is a significant part of the problem. Only a third (33%) agreed that they feel valued by the C-Suite and 28% that the value of their role is recognised by the board. The power of risk and resilience solutions to make pre-emptive and informed business decisions to drive performance can't be underestimated and as a collective we need other senior leaders to recognise this.

Becoming a voice in the boardroom.

In order to protect organisations from ongoing threats, information security leaders require the necessary budget and resources to make a difference. To achieve this, it is crucial for CISOs to have a strong presence and influence in the boardroom.

Our data indicates that progress is being made in acknowledging the significance of information security at board level discussions and with key decision makers. However, there is more work to be done to ensure that information security receives the attention it deserves.

Encouragingly, nearly three quarters (73%) of CISOs stated that their board comprehends the risks associated with information security incidents and their potential consequences. Additionally, 73% reported having regular access to the board. But this is unfortunately countered by attitudes towards information security not necessarily changing for the right reasons. A notable 78% of respondents mentioned that high-profile security incidents have led to increased budget allocation and support.

To make a shift, CISOs need to leverage this heightened awareness of business risks to their advantage. This is an excellent opportunity for security leaders to educate the board on the most critical threats and the potential business impacts of these threats if they are not addressed. Tackling the worrisome lack of buy-in from C-level executives regarding the role of information security, which nearly half (49%) of CISOs face, is essential. It is disappointing to note that a mere 9% of CISOs consider information security as one of the top three priorities on the boardroom's meeting agenda.

Such a level of prioritisation for information security is unacceptable in a world of evolving threats that can result in significant financial and reputational penalties. The situation needs to change so that there are more than the current 22% of CISOs actively participating in business strategy and decision-making processes.

It is crucial for CISOs to be acknowledged as a vital enabler to commercial operations, with information security a part of every business decision.

The way forward.

By working with partners and service providers, organisations can bolster information security defences and address CISOs top priorities and challenges without oversaturating in-house SecOps teams.

The beauty of the partner approach is that third parties can take a step back and start with a blank canvas if needed: delivering a full-scale risk management programme; helping reimagine information security resilience and recovery approaches; or working on a specific project.

In fact, many CISOs already acknowledge the value that partners and service providers deliver. Nearly half (45%) of CISOs typically engage in three-to-six-month projects with external companies, while just over a quarter (27%) engage for six months to a year.

Top benefits of a full-service risk and information security solutions provider, like BSS, include:

Taking away the pain of regulation
Each company's data portfolio and regulatory needs are unique, and it is imperative to the organisations success that everything is identified, captured, managed and analysed to develop solutions, manage risk and enable growth. No matter the requirements, BSS has subject matter experts with the experience needed to achieve any goal.

Solid information security resilience and assurance
Adaptability is key to remain operational. By working with BSS, we'll ensure security measures are effective and up to date, while identifying and mitigating risk areas that may impact business continuity. These will contribute toward forming effective information security frameworks with ongoing training.

Providing UK-based talent and skills
UK-based service providers with UK subject matter experts understand local information security, risk, assurance, regulation and compliance needs. Therefore outcomes can be managed end-to-end with local teams, and for any urgent situations, these experts are based in the same time-zone for effective, timely management of the crisis.

Optimising change management
Don't fall into the trap of assuming in-house teams can cope with every change management project. A lot of the existing security resources aren't enough to consume the additional effort required to support all necessary changes. Full service and solutions providers, such as BSS, can support as required, as well as develop long-term change management processes that enable businesses to adapt in an evolving threat landscape.

Communicating information security and investment needs to the board
By partnering with BSS' subject matter experts and former CISOs, we can help organisations to communicate and simplify the challenges and needs of the rest of the C-Suite. And for organisations that can't justify the overheads of a full CISO function, our virtual CISO services enable clients to benefit from knowledge, expertise, and guidance of experienced, accredited CISOs as and when needed.

BSS.

Solve your problems with BSS.

CISOs face complex information security challenges that are unique to their organisations. BSS understands that these challenges are distinct, and we excel at delivering tailored solutions that address your specific requirements.

With extensive experience in dealing with security and risk management challenges, our team of trusted experts are well-equipped to provide the guidance you need. Our results-oriented approach means we're committed to delivering effective solutions quickly and within your budget constraints.

We believe the most successful projects, outcomes and service provision come from good relationships, the right expertise, and clear communications. This means being up-front and realistic, while ensuring that you have a complete understanding of our processes and recommendations.

Contact us to see how we can help you.

Email: info@bss.uk.com
Call: 020 7936 8999