How to make an impact in your first 90 days as a new CISO?

An information security eBook by TSC

Raise awareness | Develop knowledge | Change behaviour | Develop security culture

Congratulations on your new role as a Chief Information Security Officer (CISO)!

As a CISO, you play a critical role in protecting your organisation's information assets and managing its cyber security risk. However, being a CISO is not an easy task, and the first 90 days in this role are particularly challenging.

In this eBook, we will share some insights and practical tips to help you make an impact in your first 90 days as a CISO and set yourself up for long-term success.

Contents

Introduction

1a. Understanding the cyber security landscape

Before diving into the specifics of your new role, it's important to understand the cyber security landscape and the challenges you'll face.

Here are some quotes from industry experts to help frame your thinking:

"The biggest challenge facing CISOs today is managing risk in an ever-changing environment." ***Richard Stiennon, Chief Research Analyst at IT-Harvest***

"The cyber threat landscape is constantly evolving, and so must our approach to cyber security." ***Chuck Robbins, CEO of Cisco***

"The most significant challenge facing CISOs is the need to align their cyber security strategies with the business objectives of their organisation." ***Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute***

According to a recent study, the average cost of a data breach is $4.24 million. The study also found that the longer it takes to identify and contain a breach, the more expensive it becomes.

Therefore, one of your top priorities as a CISO is to develop a robust cyber security strategy that aligns with your organisation's business objectives and effectively manages your organisation's cyber security risk.

1b: Key statistics: The state of cyber security readiness

Understanding the current state of cyber security readiness is essential for a new CISO.

Let's take a look at some key statistics that highlight the challenges and opportunities organisations face in today's cyber landscape:

According to a report by IBM Security, the average total cost of a data breach in 2022 was **$4.35 million,** with an average time to identify and contain the breach of 277 days.

The Verizon Data Breach Investigations Report (DBIR) found that **82%** of breaches involved a human element, such as social engineering or phishing attacks.

These statistics underscore the urgency for organisations to prioritise cyber security awareness and education.

By partnering with The Security Company, you can leverage their eLearning, games, and animations to address these knowledge gaps and enhance your organisation's overall security readiness.

1c: Assessing your cyber security posture

To develop an effective cyber security strategy, you need to understand your organisation's current cyber security posture.

Here are some steps to assess your organisation's cyber security posture:

Conduct a comprehensive risk assessment to identify and prioritise your organisation's cyber security risks.

Review your organisation's existing policies and procedures and assess their effectiveness.

Perform a gap analysis to identify areas where your organisation's cyber security posture needs improvement.

Engage an independent third-party to conduct a penetration test or vulnerability assessment to identify potential weaknesses in your organisation's defences.

The Security Company's expertise in behavioural analysis and comprehensive assessments can provide a holistic view of your organisation's security landscape.

1d: Developing your cyber security strategy

Based on your assessment of your organisation's cyber security posture, you can now develop your cyber security strategy.

Here are some elements to include in your cyber security strategy:

Develop a comprehensive incident response plan that outlines how your organisation will respond to a cyber security incident.

Establish clear policies and procedures for data classification, access control, and data retention.

Develop an ongoing employee cyber security awareness and training program to help your employees understand their role in maintaining your organisation's cyber security.

Consider implementing a security culture change program to foster a security-first mindset across your organisation.

TSC: Your partner in cyber security and culture change

As you embark on your journey to transform your organisation's security culture, partnering with a trusted cyber security awareness training and security culture change provider like The Security Company can significantly enhance your efforts.

The Security Company offers a wide range of services and products tailored to help you educate, engage, and empower your workforce to become a proactive line of defence against cyber threats.

Where to start?

2a: Building relationships

As a CISO, you must build strong relationships with your colleagues, stakeholders, and partners.

Here are some tips to help you build effective relationships:

- Communicate regularly with your stakeholders to understand their needs and concerns.
- Establish an open and transparent dialogue with your board of directors and senior management team.
- Build relationships with your peers in other departments, such as IT, legal, and compliance, to ensure that everyone is working together towards a common goal.
- Attend industry events and conferences to network with other cyber security professionals and stay up to date on the latest trends and threats.

2b: Behavioural analysis for enhanced insight

Behavioural analysis is a powerful tool that can provide valuable insights into the security culture of your organisation. By understanding employee behaviours, attitudes, and decision-making processes, you can tailor your cyber security initiatives to address specific challenges and promote positive security practices.

The Security Company's expertise in behavioural analysis can help you identify patterns, uncover areas of vulnerability, and design targeted interventions. By analysing employee behaviour, you can pinpoint potential weaknesses in security awareness and tailor training programs to address them effectively.

As Peter Drucker once said, "*Culture eats strategy for breakfast*." By leveraging behavioural analysis, you can gain a deeper understanding of your organisation's security culture and drive meaningful change that aligns with your overall cyber security strategy.

2c: Defining your strategic objectives

Defining clear strategic objectives is crucial for setting the direction and priorities of your cyber security initiatives. Your objectives should align with the organisation's overall goals and address its unique risk landscape. Consider the following when defining your strategic objectives:

- **Protecting critical assets:** Identify the organisation's most valuable assets, such as customer data or intellectual property, and develop strategies to protect them effectively.
- **Enhancing incident response capabilities:** Strengthen your organisation's ability to detect, respond to, and recover from security incidents by establishing robust incident response plans and processes.
- **Building a security-aware culture:** Foster a culture of cyber security awareness and responsibility throughout the organisation, ensuring that security becomes everyone's responsibility.
- **Strengthening partnerships:** Collaborate with key stakeholders, such as IT teams, senior executives, and external partners, to align cyber security objectives with business objectives and promote a collaborative approach.

2d: Prioritising initiatives based on risk assessment and behavioural analysis

Once you have defined your strategic objectives, it's important to prioritise your initiatives based on a thorough risk assessment. Consider the following steps when prioritising your cyber security initiatives:

- **Identify and assess risks:** Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities. Consider both internal and external factors, such as regulatory compliance, emerging technologies, and evolving threat landscapes.
- **Evaluate potential impacts**: Assess the potential impact of each risk on the organisation's objectives, operations, and reputation. This evaluation will help you determine the level of priority and resource allocation required for each initiative.
- **Mitigate high-risk areas:** Prioritise initiatives that address high-risk areas identified in the risk assessment. Focus on implementing controls, policies, and training programs that effectively mitigate these risks and reduce the organisation's overall exposure.

By leveraging The Security Company's expertise in risk assessment and their wide range of solutions, such as manager masterclasses and competency frameworks, you can ensure a systematic and targeted approach to addressing your organisation's unique risks.

2e: How to engage key stakeholders

As a new CISO, it is crucial to engage with key stakeholders across the organisation to build support and promote a culture of cyber security. By fostering strong relationships with executives, department heads, and employees, you can gain their trust, align their priorities with cyber security objectives, and ensure a coordinated approach to security.

Consider the following strategies:

- **Establish regular communication channels**: Foster open lines of communication with key stakeholders to exchange information, address concerns, and provide updates on cyber security initiatives.
- **Collaborate on risk management:** Work closely with risk management teams to align cyber security efforts with overall risk mitigation strategies and ensure that security measures are integrated into business processes.
- **Involve HR and training departments:** Engage with HR and training departments to integrate cyber security awareness and training into employee onboarding, development programs, and performance evaluations.

Let's start communicating

3a: Communicating the importance of security culture

Effective communication is paramount in establishing a strong security culture within an organisation. You must articulate the vision, goals, and benefits of a security-conscious environment to gain buy-in from employees at all levels.

Consider the following communication strategies:

Clearly define the vision:
Develop a clear and concise statement that articulates the organisation's vision for a strong security culture. Communicate this vision consistently through various channels, such as team activities, newsletters, and intranet platforms.

Emphasise the importance of security:
Communicate the potential risks and consequences of cyber threats to employees, highlighting the impact on the organisation, its customers, and stakeholders. Use real-world examples and statistics to underscore the importance of security awareness and adherence to policies.

Encourage open dialogue: Foster an environment where employees feel comfortable reporting security incidents, sharing concerns, and suggesting improvements. Actively listen to their feedback and address their questions and concerns promptly.

As Simon Sinek once said, "*People don't buy what you do; they buy why you do it*." By effectively communicating the vision and importance of security culture, you can inspire employees to embrace their role as defenders against cyber threats.

3b: Board engagement and manager masterclasses instigate leadership alignment

Manager masterclasses can play a significant role in empowering leaders to champion cyber security initiatives within their teams. The Security Company offers manager masterclasses designed to equip managers with the knowledge and skills necessary to promote a security-aware culture.

By participating in these masterclasses, managers can gain a deeper understanding of the threats faced by the organisation, the importance of security awareness training, and their role in leading by example. They can learn how to communicate security expectations effectively, recognise and address security incidents, and provide ongoing support and reinforcement.

As Jack Welch famously stated, "*Before you are a leader, success is all about growing yourself. When you become a leader, success is all about growing others.*" Empowering managers with the necessary knowledge and tools through masterclasses will create a cascading effect, ensuring that security awareness becomes ingrained throughout the organisation.

Articulating Cyber security Risks to the Board

As a CISO, it is essential to effectively articulate cyber security risks to the board to gain their support and secure necessary resources.

Here's how you can effectively communicate cyber security risks:

Use real-world examples: Illustrate the potential impact of cyber security risks by referencing recent high-profile breaches and their consequences. This helps the board understand the tangible risks faced by the organisation.

Provide context and metrics: Quantify the potential financial and reputational damage that could result from a security incident. Utilise relevant metrics and benchmarks to highlight the organisation's current cyber security posture and compare it to industry standards.

Explain the business implications: Clearly communicate how cyber security risks can impact the organisation's operations, customers, compliance, and competitive advantage. Relate cyber security risks to the organisation's broader business objectives to help the board understand their significance.

By effectively articulating cyber security risks to the board, you can secure their support, budget and resources to implement necessary security measures.

The Security Company's expertise in articulating cyber security risks and their understanding of board-level discussions can provide valuable insights and support in effectively communicating the risks to the board.

3c: Applying proven change models to communication campaigns

Implementing a successful security culture transformation requires a structured approach that leverages proven change models. By adopting established change management frameworks, you can increase the likelihood of success and minimise resistance.

Consider the following:

The Kotter's 8-Step Change Model: This model emphasises the importance of creating a sense of urgency, building a guiding coalition, and continuously communicating the vision to drive organisational change.

The ADKAR Model: This model focuses on individual change by addressing awareness, desire, knowledge, ability, and reinforcement. It provides a framework for understanding and managing individual resistance to change.

The Prosci Change Management Process: This process involves preparing for change, managing the change, and reinforcing change to ensure its long-term sustainability.

By applying these change models, you can effectively navigate the complexities of cultural transformation and ensure that your security culture initiatives are embraced by employees at all levels of the organisation.

What products and services to use?

4a: The role of security awareness training

Security awareness training is a vital component of building a security-conscious workforce. It equips employees with the knowledge and skills to identify and respond to potential cyber threats effectively. Security training should cover various topics, such as phishing awareness, password security, data protection, and safe browsing practices.

According to a study, organisations that provide regular security awareness training experience a **70%** reduction in security-related incidents.

By investing in security awareness training, such as The Security Company's eLearning solutions, you can ensure that your employees are equipped with the necessary knowledge to protect the organisation against cyber threats.

4b: Utilising eLearning, games, and animations for engaging training

Traditional training methods don't engage all employees. However, utilising eLearning, games, and animations can transform training into an interactive and engaging experience.

Here's why these approaches are effective:

- Research conducted by the University of Colorado found that using game-based learning in cyber security training can increase participants' engagement and retention of knowledge by up to 9%.
- According to a study published in the Journal of Educational Technology Systems, using animations in training materials enhances learners' understanding and retention of complex concepts.

The Security Company's eLearning solutions provide interactive modules, gamified scenarios, and immersive experiences that make training enjoyable and memorable, leading to improved knowledge retention and behaviour change.

As Albert Einstein said, "*Learning is experience. Everything else is just information.*" By utilising eLearning, games, and animations, you can create impactful training experiences that resonate with employees and drive positive security behaviours.

4c: Communicating complex concepts: The power of infographics

In the world of cyber security, conveying complex concepts and technical information to stakeholders can be a challenge. This is where infographics can be a powerful communication tool.

Here's why infographics are effective:

- Studies have shown that people following instructions with text and illustrations perform **323%** better than those following instructions without illustrations.
- According to a study by Harvard Business Review, **90%** of information transmitted to the brain is visual, and visuals are processed 60,000 times faster in the brain than text.

Infographics simplify complex information into visually appealing and easy-to-understand graphics, making them an ideal medium for presenting cyber security concepts, data, and best practices.

The Security Company's expertise in creating informative and visually captivating infographics can help you effectively communicate key cyber security messages to your stakeholders.

4d: Continual training and reinforcement

Creating a security-aware workforce requires more than just one-time training sessions. It requires a commitment to ongoing training and reinforcement to keep employees vigilant and informed about evolving threats.

According to a study published in the Journal of Information Systems Education, continuous security training reduces the likelihood of employees falling victim to phishing attacks by up to **80%**.

Regularly provide refresher training sessions and awareness campaigns to reinforce security best practices, address emerging threats, and remind employees of their role in protecting the organisation's assets.

By implementing a culture of continual training and reinforcement, you can ensure that your employees remain knowledgeable, alert, and prepared to defend against evolving cyber threats.

Final thoughts

5a: Conducting post-implementation assessments

After implementing security culture initiatives, it is crucial to conduct post-implementation assessments to evaluate their effectiveness and make necessary adjustments.

Here's why these assessments are essential:

- According to a study by Gartner, organisations that regularly assess the effectiveness of their security awareness programs experience a **40%** reduction in security incidents caused by human error.
- Post-implementation assessments allow you to gather feedback from employees and stakeholders, identify areas of improvement, and measure the impact of your initiatives on the organisation's overall security posture.
- These assessments provide an opportunity to refine training materials, update policies and procedures, and address any emerging threats or vulnerabilities.

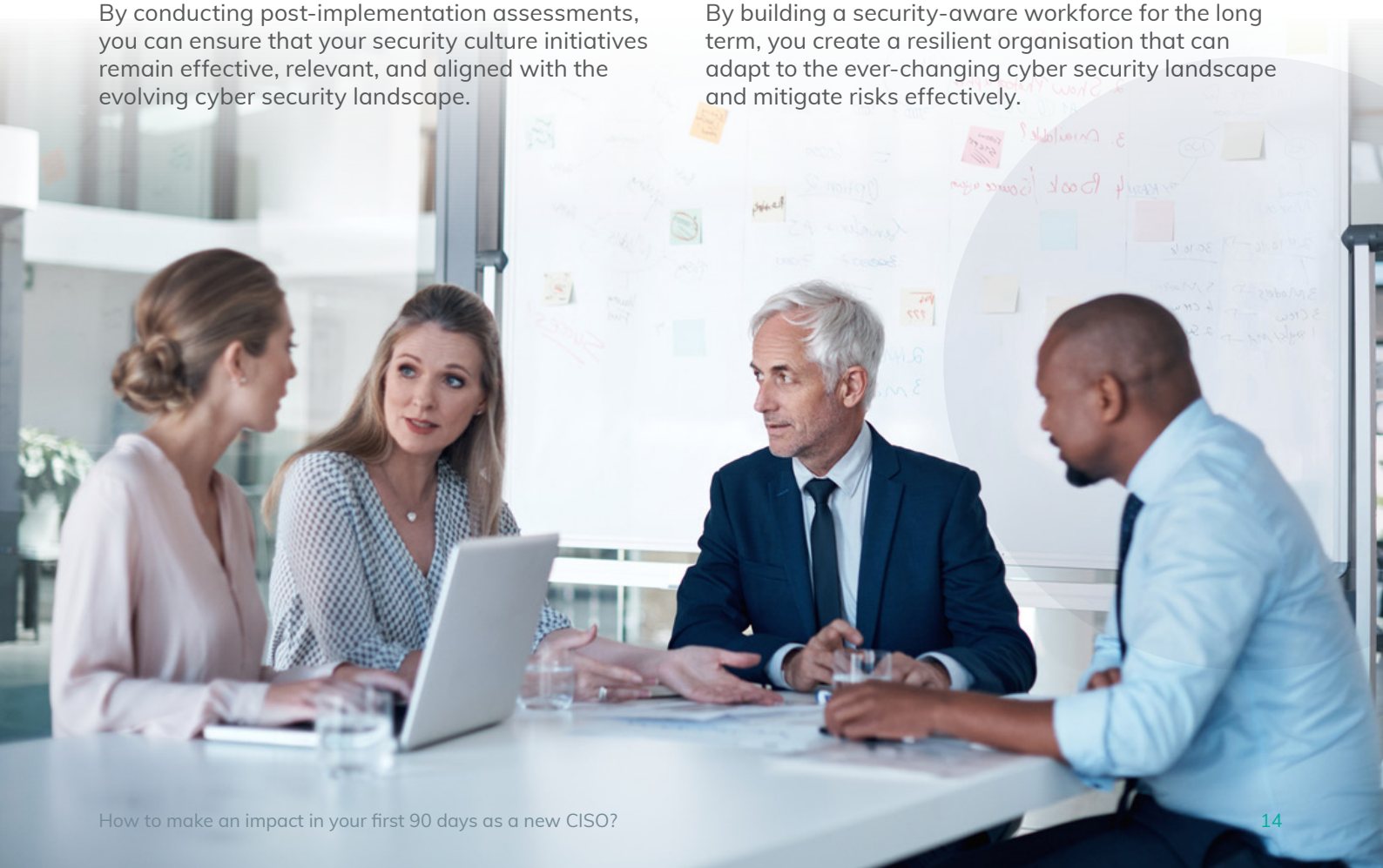
By conducting post-implementation assessments, you can ensure that your security culture initiatives remain effective, relevant, and aligned with the evolving cyber security landscape.

5b: Building a security-aware workforce for the long term

Creating a security-aware workforce is a long-term commitment that requires consistent effort and dedication. By focusing on the following strategies, you can cultivate a culture of security that becomes ingrained in your organisation's DNA:

- Foster leadership support: Engage senior executives and managers in championing security initiatives, leading by example, and reinforcing security practices within their teams.
- Encourage employee participation: Create channels for employees to report security concerns, provide feedback, and contribute to the organisation's security initiatives. This empowers them to take ownership of security and feel valued as active contributors.
- Foster a learning culture: Encourage continuous learning and professional development in cyber security by providing opportunities for employees to expand their knowledge and skills through training, certifications, and industry events.

By building a security-aware workforce for the long term, you create a resilient organisation that can adapt to the ever-changing cyber security landscape and mitigate risks effectively.



The Security Company: Your trusted Partner for long-term success

Partnering with The Security Company provides you with a trusted ally in achieving long-term success in your security culture initiatives. With our expertise and comprehensive range of services,

The Security Company can support you throughout your journey.

Here's why we are the ideal partner:

Extensive experience:

With years of experience in the cyber security industry, The Security Company has a deep understanding of the challenges organisations face in building a security-aware culture. We bring a wealth of knowledge and practical insights to guide you through the process.

Proven track record:

The Security Company has a proven track record of success, having assisted numerous global organisations, from a variety of industries, in transforming their security culture. We have received accolades and recognition for our innovative approach and ability to drive positive behavioural change.

Tailored solutions:

The Security Company offers customisable solutions that cater to the unique needs and goals of your organisation. Whether you require engaging training materials, effective communication strategies, or change management support, we can tailor our offerings to meet your specific requirements.

Comprehensive services:

From security awareness training and communication campaigns to board engagement and behavioural analysis, The Security Company offers a wide range of services to support every aspect of your security culture initiatives.

Partnering with The Security Company ensures that you have a dedicated partner committed to your organisation's long-term success in building a security-conscious culture.

In conclusion, by leveraging proven change models, conducting post-implementation assessments, providing continual training and reinforcement, and partnering with The Security Company, you can lay a strong foundation for a security-aware workforce and mitigate the risks of cyber threats effectively.

Building a security culture is an ongoing journey that requires dedication, adaptability, and the right partners. With the right strategies and support, you can create a resilient organisation that prioritises security and defends against evolving cyber risks.

www.thesecuritycompany.com @TSCPeopleSec @thesecurityco @thesecurityco