

A night photograph of a modern bridge with illuminated supports and a blue light beam. The bridge's structure is illuminated with warm yellow lights, and a bright blue light beam cuts across the dark sky from the left. The bridge spans over a body of water, with city lights visible in the distance.

CHIEF INFORMATION SECURITY OFFICER

focus > improve > achieve

fifth
STEPTM

The Need for Strategic Information Security Management

The role of the CISO has never been more important to organisations than it is today. The increase in threats from organised crime, nation states, malware, ransomware and crypto mining combined with the increased media coverage of major breaches as well as the increasing regulation means that boards of companies in all sectors are recognising the need for a CISO.

High-profile incidents involving hacking and security breaches have exposed the new reality of digital threats, and the risks they pose across the enterprise. As a result, CISO roles are branching out from being data guardians to playing a central role planning strategic risk assessments. CISOs are being embraced by senior management as business enablers. As well as identifying the risks they need to be able to embrace the information opportunities.

The role of the CISO has evolved, broadened and become better recognised in recent time, this is a direct result of increasing interest by boards caused by regulations such as GDPR (EU) and NYCR500 (USA) requiring a CISO type role. The

information security landscape increasingly plays a part in the lives of organisations that operate internationally thanks not only to regulation such as GDPR, Solvency II, MiFID II, etc. but also because of market pressures and market initiatives such as the insurance sector's Target Operating Model being rolled out by Lloyd's.

As the role of the CISO has changed, so have the reporting lines, historically cybersecurity and data privacy were considered to be firmly in the realm of IT, this is no longer the case, with CISOs increasingly reporting directly to the CEO and attending board meetings.

This is where Fifth Step's flexible data protection approach comes into its own – we provide our clients with access to senior CISO and security leadership in the way that suits them, their business need and their budget. This could be on a project by project basis (perhaps you need an information security assessment for example), or you need access to a CISO on a regular basis via our flexible and fractional CISO service (starting at on a 2-days per month basis) or perhaps you need someone full time. No matter which is your preference,

Fifth Step provides experienced CISO leaders and strategists to release the power of your information assets or fill all the security gaps in your organisation.

Evolving Cyber Threats



Making the most of your data

- Is your CISO capability changing from technical solutions to more business-orientated?
- Is a skilled, dedicated information security capability critical to the success of your company?
- How do you protect your intellectual property? Is analytical data generated by customers a potential source of competitive advantage?
- Do you know precisely how much information gold is locked away in your organisation and where is it stored?
- Have you ensured clarity in your budget forecasting and spend?
- If you took a call from senior management tomorrow asking you to prepare a report on your information security readiness would you be prepared?

Making the most of your budget and resources

- Is major business change or a recent acquisition affecting your implementation of information security controls?
- Are your Business Process Improvement specialists helping you to integrate Continual Improvement into your organization?
- What are you doing to ensure that on-going vendor support is managed and maintained?
- Is there budget or resources to bring the complex information security landscape to a supported level?
- Are you finding that there are increases in information security lapses and breaches?
- Is your business future proofed against security lapses within your market place?

Making the most of your people

- Are you flexible enough to respond quickly to ever-changing market dynamics?
- Are you able to analyze information separating the critical from the non critical?
- Is there a management process in place to support agile development?
- Do you have a people back up plan or is it all kept in the heads of your CISO or other delegated information security specialists?

The CISO Domain



Information Security Landscape Solutions

- Achieve and maintain regulatory compliance (GDPR, NYCRR500, etc)
- Ensure business is resilient in the face of the increasingly dangerous digital environment
- Implement a risk-based control structure
- Ensure that policies, processes and procedures are aligned and appropriate to their environment
- Reduce cyber-related risk
- Achieve breach readiness
- Ensure high levels of staff and organisational awareness of cyber risks and data protection requirements

The Opportunity: Competitive Advantage?



CHIEF INFORMATION SECURITY OFFICER

Data is your most valuable business asset. But how safe is it? Does everyone in your company know what risk exposure is and how to reduce it? And are they aware that they are all responsible for protecting your business? You work hard to be competitive and maintain your credibility, and your customers trust you to protect them and their interests. But this can all be destroyed with one innocent email sent with a malicious intent, or by the failure to perform a simple task. Fifth Step's flexible and scaleable CISO service is proactive, strategic and based on a strong resiliency framework. We also offer highly sophisticated risk assessment services, and will work with you to develop your own resilience culture.

Fifth Step CISOs are helping our clients to:

- Achieve and maintain regulatory compliance (GDPR, NYCRR500, etc)
- Ensure business is resilient in the face of the increasingly dangerous digital environment
- Implement a risk-based control structure
- Ensure policies, processes and procedures are aligned and appropriate to their environment
- Reduce cyber-related risk
- Achieve breach readiness
- Ensure high levels of staff and organisational awareness of cyber risks and data protection requirements

Fifth Step can help you gain a greater understanding of your data requirements and if requested, work with you and your IT team on the next phase of any work.

If you would like to learn more about the Fifth Step Chief Information Officer please contact us - info@fifthstep.com



London Office

Fifth Step Limited,
33 Queen Street,
London EC4R 1BR

Telephone: +44 (0)20 7193 1966

Email: info@fifthstep.com

US Office

Fifth Step Inc.,
1740 Broadway New York,
NY 10019

Telephone: +1 (646) 583-0085

Email: info@fifthstep.com

Bermuda Office

Fifth Step Bermuda,
Rosebank Building,
12 Bermudiana Road,
Hamilton HM11

Telephone: +1 (441) 295 3806 x206

Email: info@fifthstep.com

www.fifthstep.com

A decorative graphic at the bottom of the page consisting of numerous thin, white, wavy lines that create a sense of motion and depth, starting from the left and curving towards the right.