

Proactive data security: A strategic approach to reducing risk

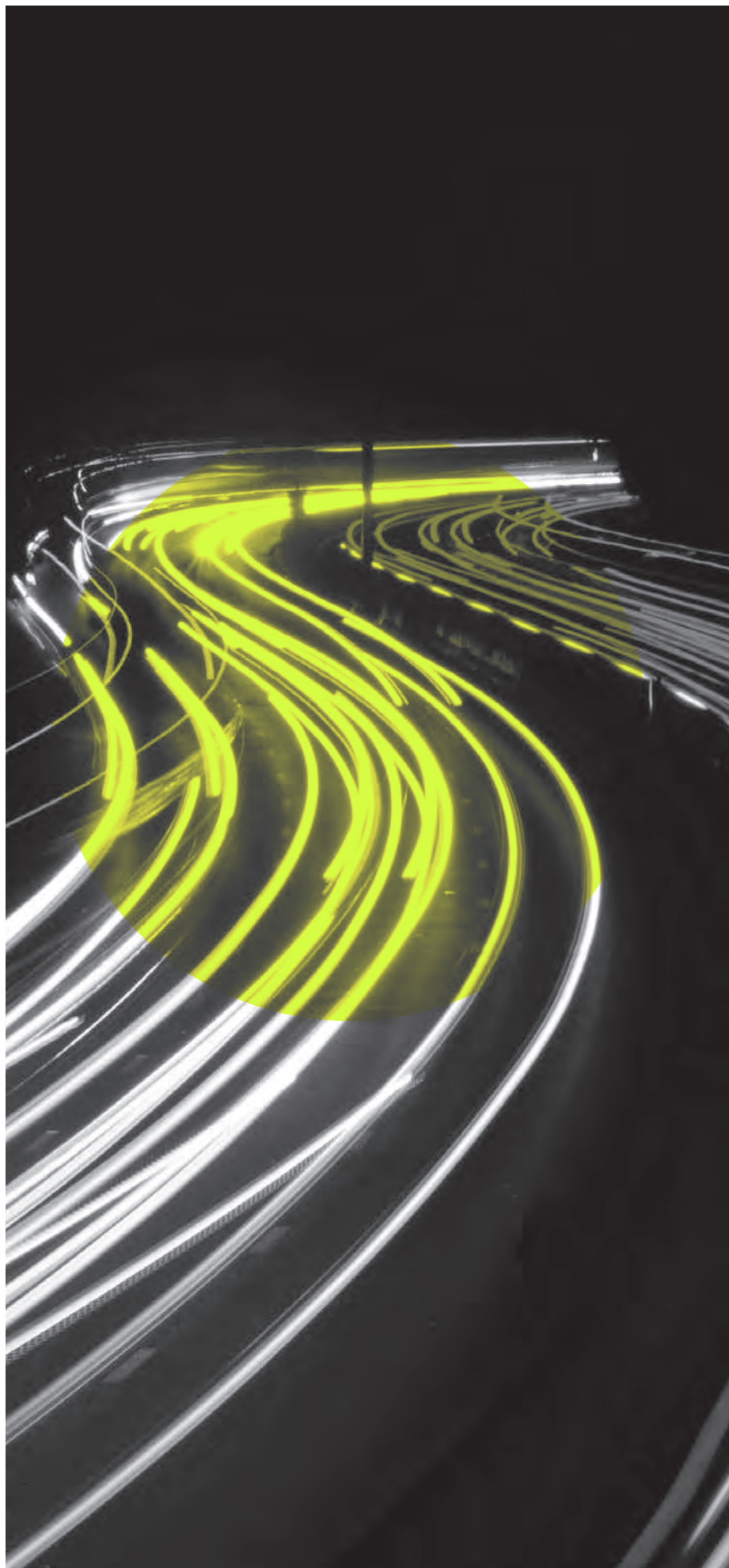
The background of the slide features a grayscale map of a city street grid. Two large, semi-transparent green circles are overlaid on the map. The right circle is larger and contains the text 'Everything you need to know about embedding a proactive data security strategy within your organisation.'.

Everything you
need to know
about embedding
a proactive data
security strategy
within your
organisation.

The evolving data security landscape

The past few years have seen significant changes in the way we work and store data, sped up by the rise of remote and hybrid work environments. These changes have introduced new challenges in data security and increased the attack surface for cybercriminals, requiring organisations to adapt their strategies to protect sensitive information effectively. Change is inevitable, but what happens when organisational processes haven't kept up? If your data is improperly managed, you can lose track of critical information and put your organisation at risk of avoidable breaches.

Failing to address data security can lead to severe consequences, including financial losses, reputational damage, and legal repercussions. High-profile breaches, such as Ticketmaster in 2024 and MOVEit in 2023, highlight the importance of staying ahead of potential threats. That's why a proactive approach is critical. Organisations that don't take proactive measures may find themselves facing regulatory fines, reputational damage, loss of client trust, and significant operational disruptions.



Understanding your data risks

Understanding where your data is and how it can be compromised is crucial for maintaining robust security. With the shift to remote and hybrid work, data is now stored and accessed across various

platforms and locations, both cloud-based and on-site, making it more challenging to manage and protect. This section delves into the key aspects of data risks, including the decentralisation of data storage,

the various ways data leakage can occur, and the significant role human error plays in data breaches. By recognising these risks, you can implement effective strategies to safeguard sensitive information.





Where is your data?

The decentralisation of data storage can lead to data being improperly managed, increasing the risk of breaches. For example, staff at one NHS Trust were using WhatsApp to share patient information and this resulted in a significant data breach, emphasising the need for robust data management practices. Within your organisation, you must have a clear understanding of where data resides—whether on-premises, in the cloud, or on employee devices—to effectively manage and secure it.

How data leakage occurs

Data leakage can occur through various means, including technical vulnerabilities and human error. Real-world examples—such as Pegasus Airlines accidentally exposing 6.5TB of data due to an AWS S3 bucket misconfiguration—demonstrate how easily data can be exposed if proper security measures are not in place. Technical vulnerabilities, such as unpatched software, misconfigured systems, and weak access controls, can also be exploited by attackers to gain unauthorised access to sensitive information.

The role of human error in breaches

It's not always technical, however. Human error remains a leading cause of data breaches. Training employees to recognise and prevent security threats is crucial in mitigating this risk. According to Mimecast's research, 74% of breaches were caused by human factors, highlighting the need for continuous education and awareness. Employees must be aware of the common tactics used by cybercriminals, such as phishing and social engineering, and understand the importance of following security protocols. Phishing assessments and training can help employees identify and correctly respond to attempted attacks to reduce the risks to your organisation.

Strengthening security measures

To protect information effectively, it's important to implement robust security measures. This includes data governance, employee training, secure configurations, and the use of Data Loss Prevention (DLP) tools. These strategies help ensure data integrity, prevent breaches, and maintain compliance with regulatory requirements.





Implementing robust data governance

Effective data governance involves regular audits, strict access controls, and encryption to protect sensitive information. You must ensure that data governance policies are up-to-date and comprehensive. Regular audits help identify potential weaknesses and ensure compliance with regulatory requirements. Access control measures, such as role-based access control (RBAC), ensure that only authorised personnel have access to sensitive data, and attackers can't pivot through a network to find what they are looking for if they do break in. Encryption protects data both at rest and in transit, making it unreadable to unauthorised users.

Training employees to be the first and last line of defence

Employees should be trained regularly on data security best practices, including recognising phishing attempts and how to handle sensitive information securely. This training should be ongoing to keep up with evolving threats. You can implement security awareness programmes within your organisation that include simulated phishing exercises, regular training sessions, and updates on the latest security threats. Empowered employees contribute to significantly reducing the risk of data breaches.

The importance of secure configurations and penetration testing

Regular configuration reviews and penetration testing are essential to identify and address vulnerabilities in your systems. These practices help ensure that your digital infrastructure is secure and resilient against attacks. Secure configurations involve setting up systems and applications according to best practices, such as disabling unnecessary services, applying security patches, and enforcing strong password policies. Penetration testing simulates real-world attacks to identify weaknesses and provides actionable recommendations for improving security.

Using Data Loss Prevention (DLP) tools effectively

DLP tools can detect and block suspicious activities, helping to prevent data breaches. Organisations should implement both technological and human-led processes to monitor and secure their data effectively. DLP solutions can monitor data in use, in motion, and at rest, providing comprehensive protection against data leakage. By setting up policies and rules, you can prevent unauthorised access, sharing, and transfer of sensitive information.

The supply chain challenge

Managing third-party risks is crucial for maintaining a strong security posture. This section explores the importance of addressing vulnerabilities introduced by vendors, steps to assess and manage vendor security, and the necessity of embedding security into procurement and contracts to mitigate associated risks.





Why third-party vulnerabilities matter

Third-party vendors can introduce significant vulnerabilities into your organisation. The Solarwinds supply chain incident illustrates how a supplier's security lapse can have widespread consequences. It is important to recognise that your organisation's security posture is only as strong as its weakest link. Third-party vendors often have access to sensitive data and systems, making them attractive targets for cybercriminals.

Steps to assess and manage vendor security

You should conduct thorough risk assessments of vendors and require them to adhere to strict security standards. Regular audits and due diligence are necessary to ensure ongoing compliance. Vendor risk assessments should evaluate the security controls, policies, and practices of third-party vendors. You can also require vendors to obtain security certifications, such as ISO 27001 or SOC 2, to demonstrate their commitment to security.

Embedding security into procurement and contracts

Security requirements should be embedded into procurement processes and contracts to ensure that all vendors meet your organisation's security standards. This proactive approach helps mitigate risks associated with third-party relationships. Contracts should include clauses that specify security requirements, incident response procedures, and the right to audit the vendor's security practices. By embedding security into procurement, you can ensure that security is considered from the outset of any vendor relationship.

The cost of a data breach

Data breaches can result in substantial financial losses, damage to your reputation, and operational disruptions. Understanding these potential impacts underscores the importance of investing in robust data security measures. Financial consequences can include regulatory fines, legal fees, and the cost of remediation efforts. Reputational damage can lead to loss of customer trust and a decline in business. Operational disruptions can affect productivity and result in significant downtime.

Incident response planning and resilience-building

Having a well-defined incident response plan is critical to minimising the impact of a data breach. Your organisation should regularly test and update its plans to ensure they are prepared for any eventuality. An effective incident response plan outlines the steps to be taken in the event of a breach, including identifying and containing the breach, notifying affected parties, and recovering from the incident. Regular testing, such as tabletop exercises and simulations, helps ensure that the plan is effective and that all stakeholders are familiar with their roles and responsibilities.

Business continuity and regulatory compliance considerations

Ensuring business continuity and compliance with regulatory requirements is essential in the aftermath of a data breach. Organisations must have strategies in place to maintain operations and meet legal obligations. Business continuity planning involves identifying critical business functions and developing strategies to ensure their continued operation during and after a disruption. Regulatory compliance requires organisations to adhere to data protection laws and regulations, such as GDPR and CCPA, and to report breaches to the relevant authorities within specified timeframes.



Implementing a proactive security strategy

Five key steps to reduce risk

1 **Conduct regular risk assessments**

Identify and evaluate potential vulnerabilities and threats to your data. Regular risk assessments help prioritise security efforts and allocate resources effectively.

2 **Implement comprehensive data governance policies**

Establish policies and procedures for managing and protecting data throughout its lifecycle. Data governance policies should cover data classification, access control, encryption, and data retention.

3 **Train employees on data security best practices**

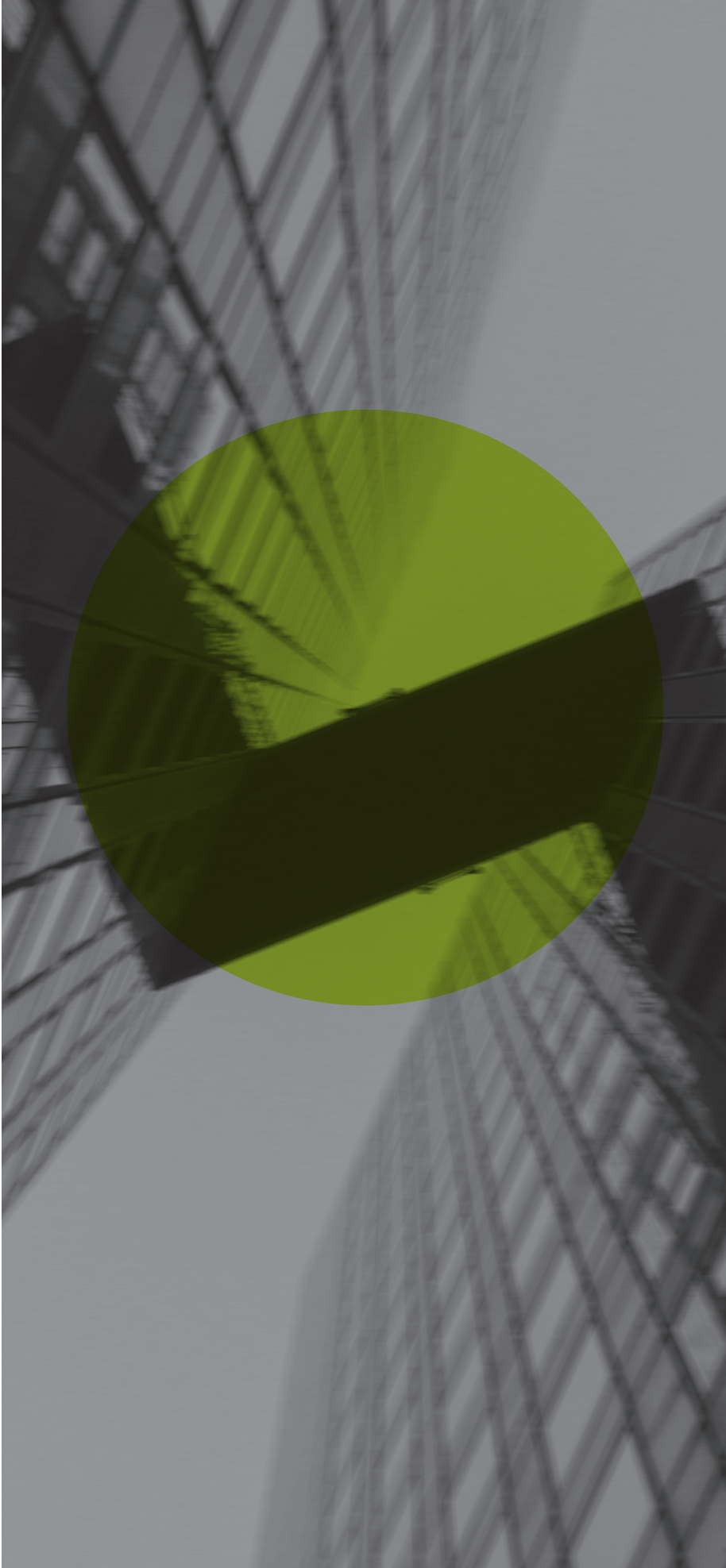
Provide ongoing training and awareness programmes to ensure employees understand their role in protecting data. Training should cover topics such as phishing awareness, password management, and secure data handling.

4 **Use advanced security tools and technologies**

Implement security solutions, such as DLP, encryption, and intrusion detection systems, to protect data from unauthorised access and breaches. Advanced security tools can provide real-time monitoring and alerting, to facilitate a quick response to potential threats.

5 **Continuously monitor and improve your security measures**

Regularly review and update security policies, procedures, and technologies to stay ahead of emerging threats. Continuous monitoring helps identify and address security gaps before they can be exploited.



The role of ISO 27001 and Cyber Essentials

Adopting recognised security frameworks, such as ISO 27001 and Cyber Essentials, can help establish and maintain effective security practices. These frameworks provide guidelines for managing and protecting sensitive information. ISO 27001 is an international standard for Information Security Management Systems (ISMS), providing a systematic approach to managing sensitive information. Cyber Essentials is a UK government-backed scheme that helps organisations protect themselves against common cyber threats.

Continuous improvement and monitoring

Data security is an ongoing process that requires continuous improvement and monitoring. You should regularly review and update security measures to stay ahead of emerging threats. Continuous improvement involves regularly assessing the effectiveness of security controls, identifying areas for enhancement, and implementing changes to address new risks. Monitoring allows organisations to respond quickly to potential threats.

Why organisations must shift from reactive to proactive security

Proactive data security is essential in today's evolving threat landscape. By taking a strategic approach to reducing risk, you can protect your organisation's sensitive information and maintain trust with your stakeholders. Reactive security measures are often insufficient to address the sophisticated and persistent threats faced by organisations today. A proactive approach involves anticipating potential threats, implementing preventive measures, and continuously improving security practices.

What can you do?

The skills required for the management of all of this may not be in-house, so you can engage with external security experts to conduct assessments and provide training. Investing in these proactive measures will help build a strong security posture and reduce the likelihood of data breaches.

Security experts can provide valuable insights and recommendations based on their experience and knowledge of the latest threats and best practices. They can help you conduct comprehensive security assessments, implement tailored training programmes, develop and test incident response plans, adopt industry best practices and standards, and implement continuous monitoring and improvement programmes.

PGI's technical and information security experts can help you move from a reactive to a proactive security posture, better protecting your data and the trust of your stakeholders. If you would like to talk about your needs, contact the team today:

findoutmore@pgitl.com
+44 20 4566 6600