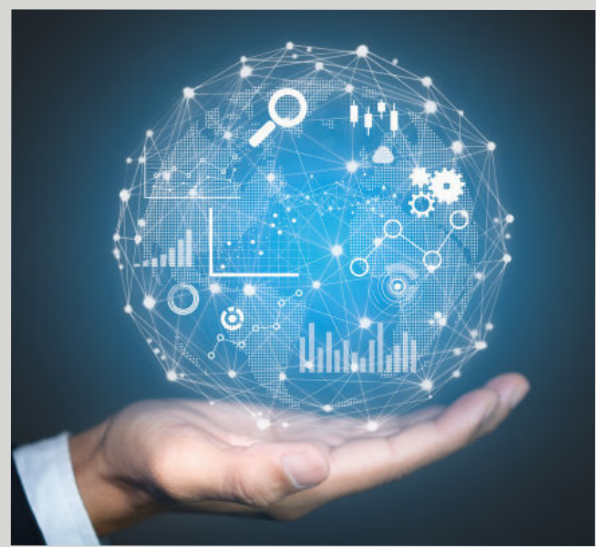




DATA DEFENCE

SHIELDING YOUR BUSINESS AGAINST CYBER
THREATS





What are the next steps in cyber protection that businesses can take?

The top priority for any business is to break free from viewing cyber security in isolation. For too long, it's been seen narrowly, without considering its interconnected components. To prevent major data breaches, businesses must adopt a holistic approach, integrating technology, organisational policies, and employee awareness.

READ ON!



How can organisations break down silos to ensure maximum effectiveness with these steps in place?

CISOs and cyber security teams must prioritise the integration of departments to enhance overall cyber security effectiveness. CISOs must assume the role of strategic partners and synchronise their objectives with broader business goals. This involves articulating in business terms to engage stakeholders and ensuring that cyber security initiatives are aligned with overarching business objectives.

With that in mind, how do CISO's and cyber security teams foster that unified approach?

A SINGLE ORCHESTRATION LAYER PULLING ALL DISPARATE TECHNOLOGIES TOGETHER

Consolidate technology and systems into one orchestration layer for continuous monitoring of an organisation's infrastructure. The strength of your technology combined will significantly enhance multiple siloed technologies.



COMMUNICATION IS KEY

Cyber security teams should eliminate technical language and promote open dialogue among teams. Painting the picture by visualising cyber risks for executive decision making is crucial. Click [here](#) to read more on painting the picture.

DEVELOP A UNIFIED CYBER SECURITY STRATEGY

Work together to develop a comprehensive cyber security strategy that aligns with the overall business objectives and addresses the specific needs of each department. Bring everyone into the conversation to foster that alliance and accountability in all.



INTEGRATE SECURITY INTO BUSINESS PROCESSES

Embed security into the organisation's business processes and workflows, ensuring that security considerations are taken into account from the outset of any new project or initiative.

The background of the slide features a dark, blue-toned image. In the center, a hand is shown holding a glowing, digital padlock. The padlock is composed of intricate circuitry and is surrounded by bright, yellow lightning bolts that crackle across the scene. The overall aesthetic is high-tech and cybersecurity-oriented.

THESE ARE THE KEY
THINGS THAT MUST
NOW BECOME A
PRIORITY IN ANY
ORGANISATION'S
CYBER SECURITY
STRATEGY:



CHECK THERE ARE STRONG SECURITY MEASURES

Run a check to ensure that you have encryption, firewalls, intrusion detection systems and antivirus software to protect your network and data.



DO THOSE SOFTWARE UPDATES & PATCHES

It's imperative you keep all software and systems up to date with the latest security patches to ensure there is no exploitation of any vulnerabilities that hackers can utilise for their benefit.



STRICT CONTROLS FOR ACCESS & AUTHENTICATION

Multi-factor authentication and strict user access will ensure that only authorised personnel can access any sensitive data.



REVIEW THE DATA YOU HOLD

Ensure that you are only holding relevant data that is necessary for operational purposes. This will limit and reduce the potential of any breach.



SECURE YOUR DATA

Use secure protocols for storing and transmitting data, such as encryption, and secure connections (e.g., HTTPS).



PERFORM REGULAR SECURITY AUDITS & RISK ASSESSMENTS

This will focus your cyber security teams on the risks your organisations hold and how to address these effectively.



ENSURE YOU HAVE AN INCIDENT RESPONSE PLAN

Review or create a comprehensive incident response plan that defines the steps that the business has to take in the event of a breach, including any legal obligations and communication protocols that have to be adhered to.



REVIEW HOW YOU MANAGE YOUR 3RD PARTIES

You have no control over the suppliers you use, however, in order to use their services, you can insist they adhere to strict security measures to protect any interconnected systems you may have.



DATA BACK UP & RECOVERY

Robust recovery plans should be in place, as well as regularly backing up any critical data; these are imperative to ensure any business continuity in the event of a breach.



REGULATORY COMPLIANCE

Stay updated with relevant regulations such as GDPR, HIPAA, or PCI DSS and ensure compliance with data protection laws to avoid legal repercussions and financial penalties.