ISCLOSURE
CYBER SECURITY

TECHNOLOGY OBSOLESCENCE

WHAT IS OBSOLESCENCE?

In an era marked by relentless innovation and rapid advancement, today's cutting-edge technology swiftly becomes tomorrow's relic. This phenomenon is not limited to hardware alone; software, the digital lifeblood of our interconnected world, is equally susceptible to obsolescence. Operating systems, applications, and programming languages evolve at a breakneck pace, rendering older iterations obsolete and unsupported.

WHAT ARE THE RISKS?

Technology and software obsolescence is a critical concern in today's rapidly evolving digital landscape. As technological advancements continue at an unprecedented pace, older hardware and software quickly become outdated and vulnerable to security threats. This obsolescence not only affects the efficiency and compatibility of systems but also poses significant security risks. Outdated software may lack essential security patches and updates, making it an attractive target for hackers and cyberattacks.

Obsolete technology and software not only impact system efficiency and compatibility but also bring about significant consequences, such as financial losses, reputation damage, legal liabilities, and regulatory penalties. Moreover, breaches resulting from obsolescence can disrupt operations, erode customer trust, and compromise sensitive data, leading to long term harm for organisations.

HOW CAN YOU MITIGATE THE RISK?

To mitigate these risks, organisations must stay vigilant, regularly update their software and hardware, and implement robust cybersecurity measures to safeguard sensitive data and maintain the integrity of their digital infrastructure in an ever-changing technological environment.

In addition to technical measures, organisations must also educate their employees on cybersecurity best practices. Employees should be trained on how to detect and avoid potential threats, such as suspicious emails or links. By creating a culture of cybersecurity awareness, organisations can minimize their risk of a cyber attack and maintain the integrity of their digital infrastructure.

HOW CAN DISCLOSURE HELP?

Disclosure have created a security service to directly address this issue. From its inception in 2017, we have offered a governance methodology service that encompasses people, process and technology. Accompanying the advice from our team, we also provide our own CISO-as-a-serice platform CyScan.

CISO-as-a-Service directly addresses the shortfall of skilled security leaders and their associated costs, providing organisations with a simple to consume, cost effective service, right sized and optimised for their needs.

We differentiate ourselves by providing concise and actionable recommendations, dramatically reducing the time taken to resolve vulnerabilities. From the initial onboarding, organisations benefit from an optimised approach that traverses the following key stages:

Assess - Full end-to-end visibility of the operational environment. Through vulnerability, posture, technical and source code assessments, Disclosure defines, identifies, and classifies the security vulnerabilities in the organisation's environment.

Secure - Our experienced security consultants work with our clients to strategise, plan and execute a viable information security program, by providing clear and concise guidance on the steps necessary to improve people, processes and technology.

Monitor - Proactively respond to security incidents and avoid breaches with a continuous holistic view of the business environment using our SIEM (Security information and event management) system.

At Disclosure, we understand that the technology landscape is constantly evolving, and with it comes new security risks and vulnerabilities. Our team of experts is dedicated to staying ahead of the curve and ensuring that our clients are protected from the latest threats.

Whether it's implementing the latest encryption standards or conducting regular vulnerability assessments, we work tirelessly to ensure that our clients are secure. We believe that transparency and communication are key to a successful security strategy, and we strive to keep our clients informed of any potential risks.

GIVE US A CALL OR BOOK A DEMO HERE

WHO ARE DISCLOSURE?

Disclosure CyberSecurity Limited ('DCS' or 'Disclosure') is a specialist cyber security company, formed by experienced consultants with extensive knowledge and wide exposure in the cyber security market. We have the breadth and depth of experience to think differently about what really needs to change in a cyber security environment to make our clients more secure and most importantly we have the proven ability to implement this change.

At Disclosure we understand that cyber security is a critical aspect of any modern business. In today's digital world companies are facing an unprecedented situation; the compromise of a cyber-attack is just a "mouse click" away. It's a matter of when, not if, an attack will take place. All organisations, no matter of their size or vertical, are at risk as the cyber criminals are deploying the latest tools, methods and artificial intelligence technologies to automate their concentrated attacks. Continually probing for the weak points in cyber defences, learning and adapting their attacks until they finally succeed!

CYBER ESSENTIALS PLUS

Disclosure currently possesses a vast range of cyber security accreditation.

Our guidance, expertise and technology will assist in the acquisition of a variety of Cyber Security Certification for your Business.

FIND OUT MORE

Information Security Management System ISO 27001 Certified

CREST

CONTACT US

☎ +44 7903 565 861

✉ info@disclosurecybersecurity.com

X @ disclosurecybersecurity

in / disclosurecybersecurity

Disclosure Cyber Security (UK&I)
Basepoint
1 Winnal Road
Winchester
SO23 0LD

Disclosure Cyber Security (EMEA)
4 Protea Place
Sandown
Gauteng 0001
South Africa