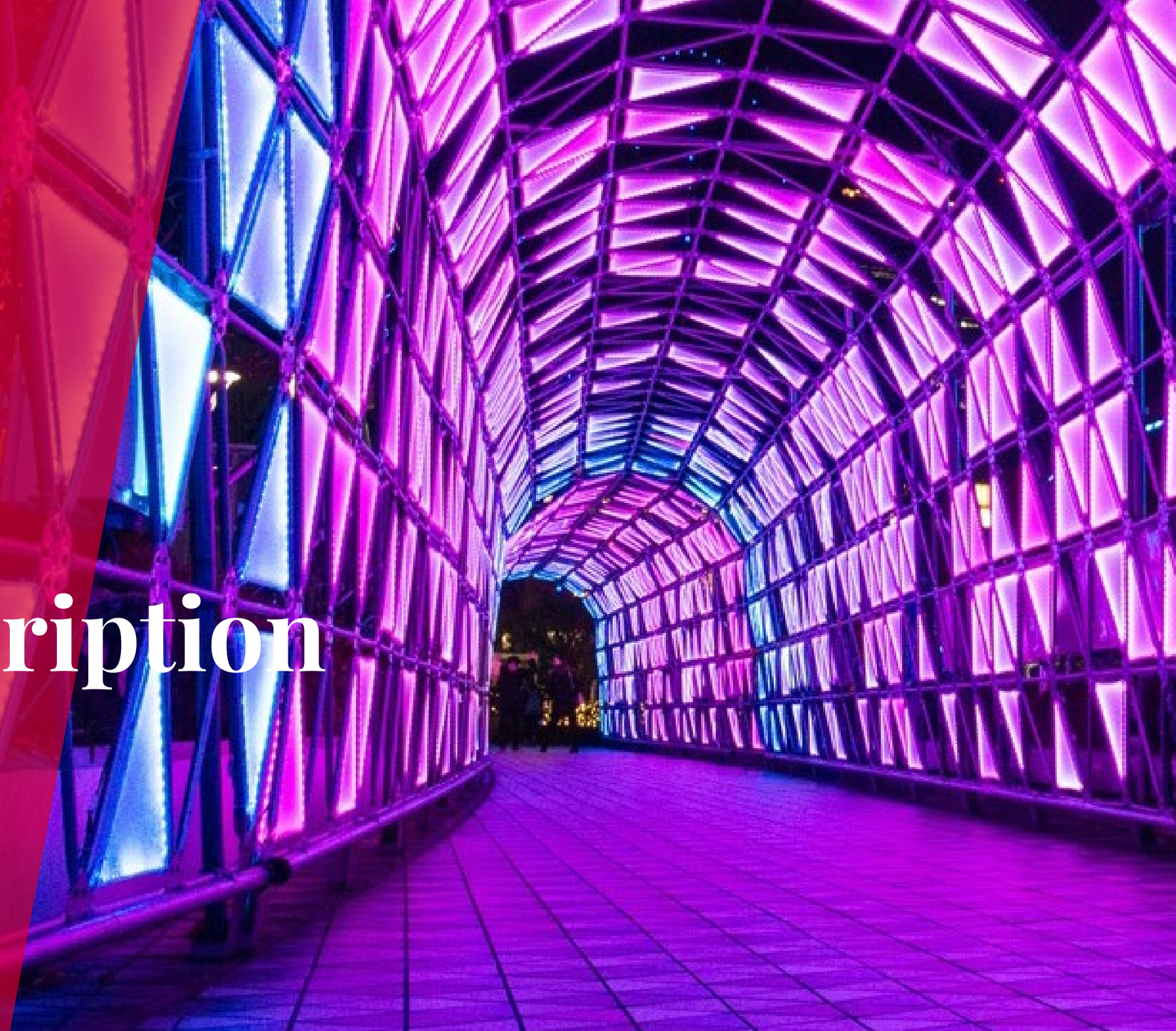
Cambridge mc²
Management Consulting

Service Description

Cyber Security



Contents

A structured guide to standardise Cambridge MC's approach to engagements, ensuring consistency and quality in service delivery.

Cambridge mc² Management Consulting

Contents

A structured guide to standardise Cambridge MC's approach to engagements, ensuring consistency and quality in service delivery.

Cambridge mc² Management Consulting

Risk and
Change Evolution

The potential of AI

to disrupt, increase efficiencies and reduce the need for paper qualifications

Organisational culture

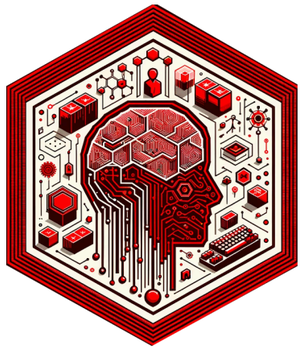
the changing nature of work and the hybrid workplace

Organisations are struggling to cope

Technology, Cloud and Data complexity

and increasingly connected devices

The Hidden Crisis in the Boardroom



These Cyber Threats bring huge potential for creating devastating commercial trauma :

- Economic Impact
- Ransomware Attacks
- Data Breaches

Cambridge mc² Management Consulting

Cambridge mc² Management Consulting

The Threat

"Cybercrime is the number one problem for mankind, and cyber attacks are a bigger threat to humanity than nuclear weapons"

WARREN BUFFET

A Growing Threat Landscape

It is no longer a matter of IF, but a question of WHEN

Global Economic Impact

Cybercrime is seen as the single greatest threat to the global economy over the ensuing decade

The World Economic Forum (WEF) states that cybercrime has emerged as the world's third-largest economy, trailing only the United States and China

Cyber Crime – Dark Web Growth

Europol data supported by NSCS suggests 300% growth in the dark web, the majority of which is now Ransomware and Malware as a Service (RaaS and Maas). It’s never been easier for cyber criminals.

Cyber security Ventures suggest a business is affected every 11 seconds.

Data Breaches

85% of cybersecurity professionals attribute the increase in cyberattacks to the use of generative AI by bad actors

Over 4.5 billion records were exposed in the top 10 data breaches alone in 2022

Alarming Disconnect: Chief Information Security Officers (CISOs) and Board members differ in confidence significantly

Disconnect

CISOs are struggle to communicate the commercial threat and Cybersecurity investments needed to Senior Decision Makers

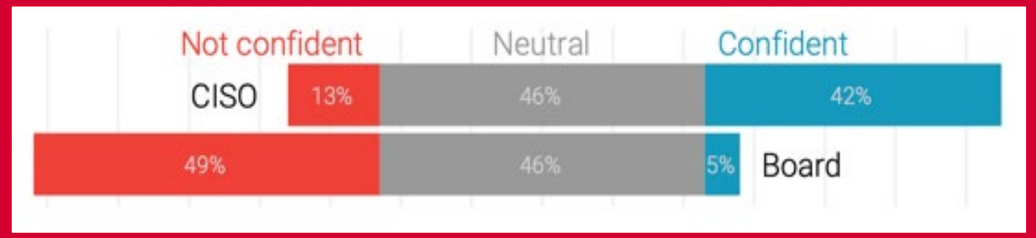
Communication

Because Cybersecurity measures and performance indicators do not often map to strategic initiatives, board members struggle to understand the commercial relevance of the reports.
Board members seek information through stories they can relate to.

CISOs therefore need support to better communicate to the board.

RECENT SURVEY REPONSE:

Q. Are you confident with the security program's effectiveness?



Cyentia Institute

Business Focus

"The board is listening and security mumbles"
""Nobody cares how many packets your firewall blocked. If security reporting doesn't reflect business goals, you're doing it wrong."

Gaining Clarity

"Tell me a story and then back it up with a few numbers."

Critical Alignment

"The things cited by Board members as most critical fell dead last among CISOs."

Cambridge mc² Management Consulting

The impact of this to you is…

Increased Commercial and Reputational Risk Exposure through….

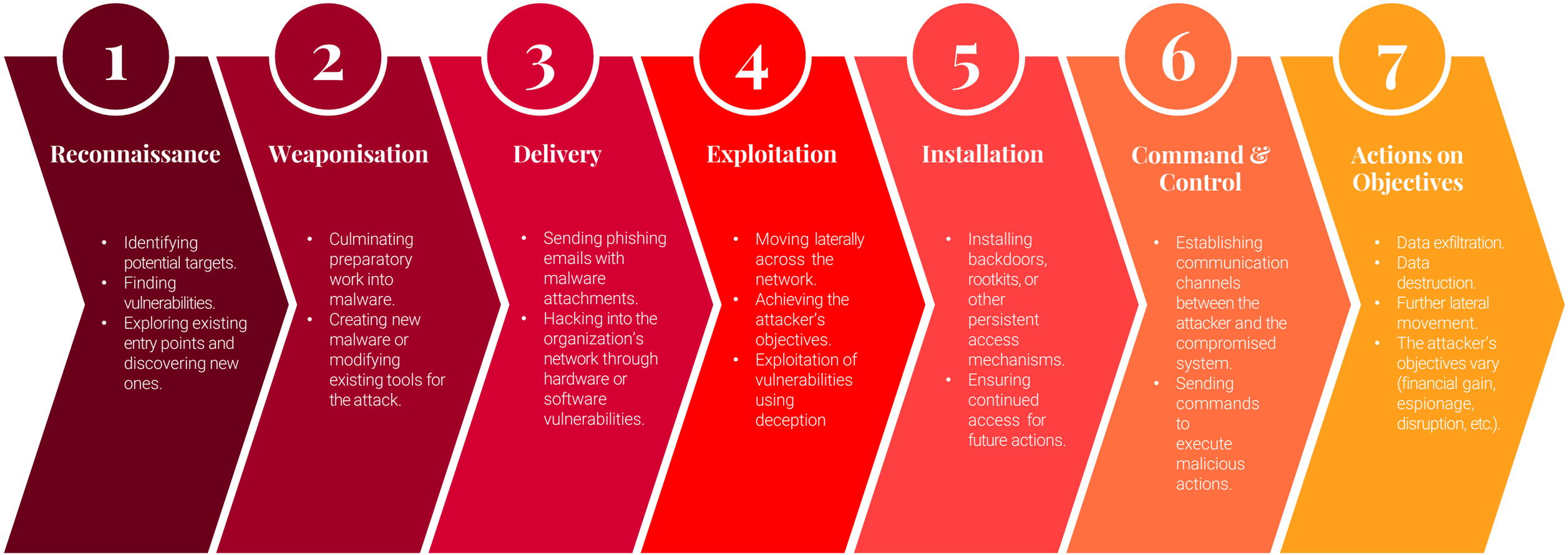
- Disconnect between commercial risk and investment in cybersecurity readiness and response
- Poor board level understanding of the widespread material impact on their cost base and reputation caused by Cyber crime
- Deep rooted cybersecurity risks due to reliance on third-party vendors and partners
- Employees inadvertently causing security breaches through actions, errors and omissions
- Ineffective monitoring, resulting in not knowing when they are compromised
- If compromised, lack of comprehensive incident response plans
- Poor understanding of and applying evolving Cybersecurity defence standards, governance and regulations (i.e NIST 2.0) within an increasingly complex technology landscape

Cambridge mc^2
Management Consulting

Cambridge mc² Management Consulting

Understanding the Attack Chain

There are seven key stages that attackers move through as they target networks and exploit vulnerabilities; understanding them re-enforces the basics.



Cambridge mc² Management Consulting

15 Signals to Show they're in your House

1 Reconnaissance

Patch Window
Known-time-to-fix etc
Vulnerability type (adds downstream exploit method, attack timeline, expected behaviour intelligence)

Web Shell
JPG file POST Parameter Requests (indicates attackers installing a webshell, like good old-fashioned SQL injection)
Length of time of login

2 Weaponisation

3 Delivery

Abnormal Logins
Patterns, Originators, brute force attempts etc including device authentication.

PIM Behaviour
Patterns, frequencies, tasks, Source, Roles, especially Admin users, with focus on privilege level role and job duties.

WMI anomalies (Windows Management Administration this is a native piece of Windows tooling allowing Administrators to do things like _InstanceCreationEvent, or _ClassCreationEvent etc the sort of stuff perpetrators will do to hide tracks or activate things.

4 Exploitation

Internal Recon
Scripts running on email, web or file servers or domain controllers (DC).
Queries listing all Service Principle Names in the DC
Windows scheduled tasks collecting stuff

Malware signals
Attempted run propagation (Malware needs to run)
Systems, files, devices, network services pinging the same host over a short period (indicates phishing or users pinging links with malware returns)
System File Device activities out of hours
Attempted comms with non-standard IP addresses
Processes modifying systems

Unusual Logs
Any event logs removed!

5 Installation

Ransomware signals
New .pky files installed (public encryption keys! Or .eky private keys..)
.res files installed (these are C&C comms)
Deletion of Backup Files

Malicious Powershell
Anomalies in commands/scripts/output
Logging anomalies (module, script block, and transcription)
Abnormal users running scripts..

RDP Signals
Remote Admin tool anomalous use

Server Message Block
Remote file management anomalies. Allows remote management of files, file-sharing, printing, directory sharing, and network stuff.

6 Command & Control

C&C Comms
N/W traffic baseline should be established, and anomalies picked up.
User Device, times, patterns

Internet Control Message Protocol (ICMP) Packets
Comms enabling packets between servers.. so once again, size and frequency is a very clear red flag of exfiltration for large volumes of unexpected or non-standard traffic.
Large packets moving!!

Hidden Tunnels
HTTPS or DNS for dry run?
Traffic baseline thresholds!

7 Actions on Objectives

Cambridge mc² Management Consulting

The Cornerstones of Cyber Exposure

The main causes of CyberCrime are not arcane Cyber details, but basic IT good practice and hygiene – such as keeping technical debt to a minimum and architecting with a “zero trust” and “Secure by Design” aprpoach

MFA

Significant improvement in systems can be gained by extending Multi-Factor Authentication (MFA) across all systems and all access requests

Privileged Access Management

Mitigate risk of breaches by restricting access to critical systems and data caused by privilege sprawl from 'authorised' personnel

Monitoring

The overwhelming output from modern security monitoring has surpassed human manageability, creating an urgent need for a streamlined, IT-integrated approach that balances automation with human oversight

End-Point Protection

The explosive growth of sophisticated, interconnected applications amplifies the pressing need for enhanced protective measures.

Application Layer

The surge in cloud migration and complex API integrations underscores the urgent need for enhanced application layer protection

Offline Back-up

Offline back-up is an essential but often underutilised strategy, providing a crucial safety net for data recovery

Contents

A structured guide to standardise Cambridge MC's approach to engagements, ensuring consistency and quality in service delivery.

Cambridge mc² Management Consulting

What customers want

Cambridge mc² Management Consulting

- To reduce commercial and operational risk
- To know their business is protected by placing knowledge from Master Practitioners into their cybersecurity defences
- Maintain reassurance that current spend level and allocation of cyber related activities represents value for money
- Confidence in the measures and actions needed to insure their organisation against material loss
- To address the real challenge of converging Security and IT to put in place the basic IT disciplines that ensure you are not first in line for compromise
- A plan that orchestrates their organisation's legal, regulatory, and reputational protection
- Gain a detailed assessment of the financial costs and business impacts of a major cyber-attack or data breach in their organisation
- A security-first approach that ensures their people Cyber security aware, and are delivering continuous risk management, compliance, and cyber security best practices which are integrated throughout their organisation and its change initiatives

Why customers like working with us

Cambridge mc² Management Consulting

- **Expertise-Driven Approach:** Our people are master practitioners in Cybersecurity – true deep practitioners with real-world experience in advising both the private and public sectors and in dealing with complex network-based cybersecurity challenges.
- **A Focus on Secure-by-Design:** Customers gain from Cambridge MC as a leader in the 'secure-by-design' approach. This involves integrating security at every stage of IT advisory, development, and operations, rather than treating it as an afterthought. We help clients build security into their IT infrastructure and business processes from the ground up.
- **Thought Leadership:** We will host webinars, workshops and are active contributors to to Government, Cyber Research, and Academia, the Security Awareness Special Interest Group.
- **Customized Cybersecurity Roadmaps:** Cambridge MC develops customized cybersecurity roadmaps for clients, considering their specific business models, industry challenges, and risk profiles.
- **Client-Centric Service Model:** Cambridge MC seeks a close collaborative relationship with our clients with respectful directness pointing out areas of basic weakness that need re-enforcement – including regular updates, transparent communication, and flexible engagement models tailored to each client's needs.
- **Strong Focus on Compliance and Regulatory Frameworks:** Given the increasing importance of data protection and privacy laws, and movement towards individual liabilities for Executives and CISO's (including possible jail terms) - Cambridge MC offers specialized services in compliance and regulatory frameworks – helping customers to navigate the complexities of GDPR, Schrems, NIS, and other relevant regulations.

Cyber Frameworks such as NIST, ISO27001 etc

How we partner with our clients

Delivering

- Confident Strategic Planning
- Effective Business Resiliency
- Clarity in Legal and Commercial Governance
- Robust Technical Solution Delivery
- Non-disruptive Project Management

A security-first approach ensures that risk management, compliance, and cyber security best practice are integrated into project management throughout.

Contents

A structured guide to standardise Cambridge MC's approach to engagements, ensuring consistency and quality in service delivery.

Cambridge mc² Management Consulting

How We Partner

Placing Our Expertise Into The Heart Of Our Client's Organisation

Assessment

Create mutual assessment of cyber risk to their organisation

Current strategy and plans to mitigated against these

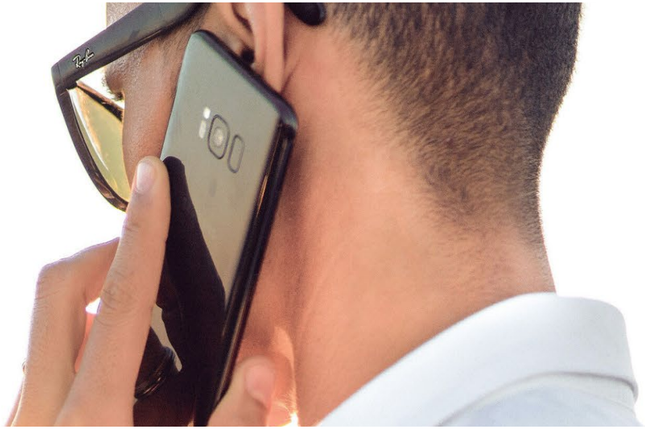
Scope and Delivery

Lead and Facilitate a comprehensive cyber security strategy and delivery plan

Partnership

Form a close/robust partnership to protect our client's organisation using leading our cyber security experience and solutions

Our Cyber Frameworks



Cyber Executive Advisory

Board-Level and Security Leader (CISO) Advisory

Ensuring your organisation's security framework is both robust and forward-looking by bridging the gap between your Board and Security Leadership (CISO)

1 day – 3 months

Cyber Accelerators

Cyber Maturity and Gap Closure

Creating a clear maturity score and actionable insights for resilient security practices by assessing your current landscape to identify gaps and areas for improvement,

2 - 4 weeks

Tailored Cyber Services

A full suite of advanced Cyber Security solutions and safeguards

Fortifying your defences and aligning them with your core objectives, by applying key insights to improve and protect your operations.

6 weeks +

Cyber As A Service

Experts on Demand

Access expert practitioner support, tailored to both your everyday needs as well as project-specific requirements, using our flexible approach to enrich and improve your Managed Security Services

12 weeks and beyond

Board Level Security Advisory Pathway Discussions

Securing Your Organisation

Cambridge mc² Management Consulting

01. Finance
The financial toll of cybercrime – digging a little deeper.

02. The Dark Web
Cybercrime's breeding ground; size and shift.

03. Incidents
Notable incidents; Optus snapshot.

04. Crises
The hidden crisis in boardrooms.

05. Government
Global Government response to cyber threats; profession and collateral.

06. Action
The urgency to act. What we can do about it.

Contents

A structured guide to standardise Cambridge MC's approach to engagements, ensuring consistency and quality in service delivery.

Cambridge mc² Management Consulting

Case Study

Cyber Security

Outcomes have been updated.
Why did the customer choose Cambridge – What did they actually say?
What Actions tangible benefits did the Institution gain by taking actions based on our recommendations?

Cambridge mc² Management Consulting

Problem

The primary challenge was the institution's realisation that its existing cyber hygiene practices and IT discipline might not be sufficiently robust to withstand increasingly advanced tactics employed by cybercriminals and their growing interest in the education sector.

The institution sought out Cambridge MC to identify these vulnerabilities, assess the overall maturity of its cybersecurity practices, and recommend strategic improvements. This meant not only highlighting technical deficiencies, but also providing a holistic evaluation of the institution's security posture, considering the practical realities of defending against threats. This included an assessment of the institution's risk readiness, infrastructure resilience and staff preparedness.

Cambridge MC's goal was to ensure that the recommendations produced as a result of this assessment were not only technically sound but contextually appropriate and aligned with the institution's strategic objectives and resources constraints. This personalised approach was crucial in designing a cyber security strategy that was both achievable and sustainable.

Approach

What we did: Our approach involved a thorough assessment of the institution's cyber infrastructure, including tests, interviews, and the examination of artifacts to gain a holistic understanding of their cyber maturity. To do this, we engaged experts with significant technical depth and extensive experience in cyber defence and leadership roles; a blend which was crucial in conducting a maturity assessment that focused on pragmatic gap closures.

Why we did it this way: Our methodology was designed to move beyond mere technical details and address the practical aspects of cyber security. By organising our work into recognised capability categories, we targeted areas that, if weak, would likely lead to vulnerability and a high risk of attack. This approach allowed us to pinpoint critical gaps in the institution's cyber security practices and propose target improvements.

Concepts and methodologies applied: We applied a risk-based approach, sensitive to the institution's risk appetite, to make practical trade-offs between cost, risk, and investment. This ensured that our recommendations were contextually appropriate and aligned with the institution's strategic objectives. Our assessment framework was grounded in industry-best practices and standards, tailored to the unique needs and challenges of the academic sector.

Obstacles encountered and overcoming them: One of the main obstacles we encountered was resistance to change, a common challenge for institutions with established routines and cultures. To overcome this, we emphasised the importance of cyber hygiene and IT discipline through clear, evidence-based findings and recommendations. We conducted workshops and discussions to engage stakeholders at all levels, highlighting the tangible benefits of enhancing their cyber security posture and demonstrating how our recommendations could be implemented in a manageable manner.

Outcomes

Optimised Cyber Resilience: The Institution gained deep knowledge of the challenge of managing over tens of thousands of accounts for a community of many fewer staff and students. Our recommendations outlined a robust workflow and identity management system across all of the institution's systems, emphasising the need for multi-stakeholder cooperation.

Longevity: The Leadership were able to agree upon specific changes which would be in place for the next three years. This was based on our clear, actionable recommendations describing implementation plans for changes, such as improving security culture and some operational deliverables associated with SOC efficacy.

Personnel Readiness: The security awareness and training of the staff, postgraduate researchers, and students, including specialised training for the Information Security team were enhanced. Our recommendations also enabled improving security posture, such as the adoption of Cloud Access Security Broker (CASB) and Data Leakage Prevention (DLP) solutions, and the development of a quantitative risk forecasting methodology.

Forward Planning: New initiatives targeting cyber kill chain strategy areas, and planning disaster recovery tests for ICT systems were created by the Institute. Our recommendations also enabled future improvements, including SOC operational activities.