COMMERCIAL FEATURE

Time to grow up: why cybersecurity maturity is crucial for organisations

A true analysis of cybersecurity can show organisations where they are at risk and measure the return on investment of cybersecurity spending

IMPORTANCE OF CYBERSECURITY MATURITY

Achieving cybersecurity maturity (CSM) enables the IT security team within an organisation to report on the status of their organisation's security posture with confidence. Through consistent monitoring and risk analysis, a clear perspective can be provided to the board. A high level of CSM is also proven to reduce overall cybersecurity spend over a three-year period.

CNS Group, an independent cybersecurity consultancy, has developed Aegis, a comprehensive CSM service. The service provides organisations with a concise and contextual reporting mechanism for cybersecurity to the board and other stakeholders. By expediting CSM and visibility, organisations of all sizes can show return on investment from cybersecurity spend, and eradicate unpredictable and ineffective spending.

WHAT IS CYBERSECURITY MATURITY?

CSM is the effectiveness of an organisation to make cybersecurity decisions in a way that considers all relevant factors on a changing technology and threat landscape; the ability to improve defences continuously while the business operates and transforms. Organisations that invest in creating a concise and accurate view of their cybersecurity state and can communicate this clearly with the rest of the business see the benefits in terms of confidence and more informed, collaborative decision-making around the value of cyber-investment.

CYBERSECURITY CHALLENGES

01 **Complexity of information for the client**

From threat intelligence, compliance and regulations to security-testing and audits, the amount of information that an organisation is required to digest and base investment decisions on is growing. Not only does this impact the level of resources and skills required from the internal IT team, but it is confusing for the extended team of stakeholders. The maze of information and limited visibility across the overall IT infrastructure can leave an organisation vulnerable.

02 **Unpredictable and ineffective spending**

With no clear reporting model, organisations are basing their investment decisions on the results of the latest penetration test, security audit or pressure from existing or new regulations in force. This never-ending project-based model doesn't allow for continuity and intelligent spend over time. The traditional cybersecurity spend becomes a pattern of testing, part-fixing, requesting more budget, spending budget, testing – and repeat.

03 **Confusing and growing compliance landscape**

From the European Union General Data Protection Regulation, PCI Security Standards Council compliance, Cyber Essentials to ISO standards, the compliance landscape is a minefield for any organisation. Although achieving compliance enables organisations to achieve a level of best practice and is a helpful negotiation tool for budget requests, it doesn't mean that an organisation is completely protected. The constant changes in regulations also require up-to-date knowledge and skills within the IT team.

MEASURING THE CURRENT STATE OF CYBERSECURITY MATURITY

There are a few variations and grading scales for measuring CSM with the most common being the COBIT maturity scale. Recent research using the COBIT scale found that only 22 per cent of IT security professionals surveyed believed their CSM level to be optimised. Almost 20 per cent stated their level of maturity as non-existent, ad-hoc or didn't know.

This growing lack of control and visibility directly impacts how informed and prepared an organisation is to deal with either attempted or successful attacks. If a chief information security officer (CISO) wants to have an informed business conversation with their executives about risk, they need the same level of confidence in their presentation of cyber-performance data and reporting as the finance director would have in the numbers they bring to the board.

AEGIS: A COMPREHENSIVE CYBERSECURITY MATURITY SERVICE

A change is required in the way we manage and report on cybersecurity and CSM offers the most effective way to manage that change. To simplify CSM for organisations and support a higher level of CSM, CNS Group developed Aegis.

Aegis is a CMS transformation programme incorporating a proprietary benchmarking tool, active dashboard and consultancy services. CNS Group specialists use the programme to support organisations in measuring and scoring their current CSM against five key domains and 73 sub-domains.

This intelligence then provides the contextual, prioritised transformation plan for the organisation to reach its cybersecurity goals. The Aegis CSM scale draws measurements from standards including: ISO 27001; Cyber Essentials (Plus); PCI DSS; SANS/CIS/CPNI – top 20 critical control set; Sarbanes Oxley; SEC OCIE; and NCSC HMG IA maturity model and risk management principles.

The CSM market remains immature. CSM dashboards often omit one of the critical components that CNS Group's Aegis platform measures or fail to provide automated, systemised reporting for elements such as penetration-testing outputs or threat intelligence. Many solutions have their own reporting function, which may or may not be reviewed regularly, their own vendor point of contact, owner, interface into the business and assigned budget. The result is impenetrable complexity with multiple vendor conversations, stressed management overhead, conflicting advice due to limited context, and an increasing number of gaps, crossover and duplication.

The Aegis programme enables organisations to standardise and automate as much data input as possible. It gives organisations a clearly defined dashboard of business metrics to articulate cyber-risk and benchmark cyber-technology, resources and investment. This form of analysis and reporting drives better, more informed cyber-conversations with every stakeholder in the business, especially at board level.

Organisations that invest in CSM can all confidently answer these questions: Compliance and accreditation: are we meeting all mandatory regimes and standards? Technical compliance: where are the vulnerabilities and poor controls in our infrastructure, and what are we doing about them? Transformation and maturity: what's our current status across all projects? Events, alerts and threats: how good is our internal and external threat intelligence? Governance and policy: how robust is our policy compliance; where are the exceptions and who owns what?

Using an agreed benchmarking process allows CISOs, IT security managers and chief information officers to create a contextual plan of action, track and share improvements, and report concisely on the value and impact of every investment. At CNS Group, we have seen the positive impact of the transformation in CSM demonstrated through better targeted investment, more robust compliance and effective allocation of resources.

The graph demonstrates how an organisation can and should drive value from its cybersecurity spend. The Aegis programme is proved to reduce cybersecurity spend over a three-year period.

CNS Group's comprehensive CSM service enables organisations to transform the quality and value of short, medium and long-term planning and decision-making. The primary benefits of Aegis aim to provide a concise and contextual reporting mechanism for situational cybersecurity to the board and stakeholders; expedite a client's CSM and visibility; show return on investment for cybersecurity spend; organise and prioritise future cybersecurity spend for greatest risk reduction; highlight the greatest areas of cybersecurity weakness for immediate action; identify greatest threats to an organisation by type; and reduce a client's overall cybersecurity spend over three-year period.

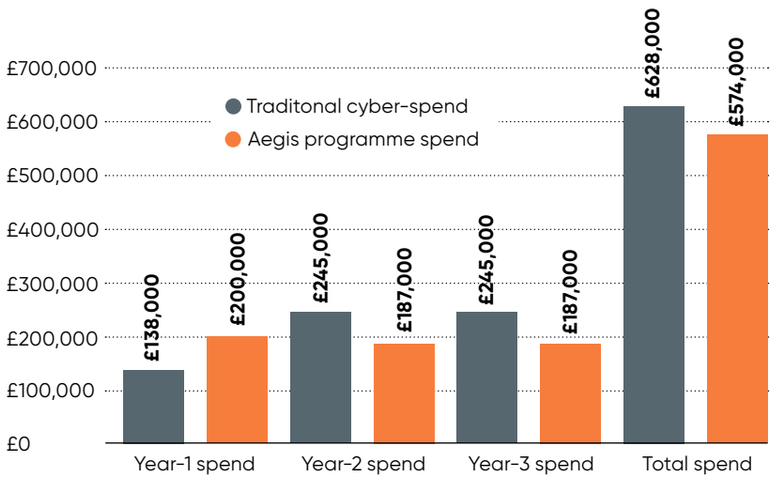
In addition, the CSM service allows organisations to identify the key and common criteria for successful cybersecurity by customer and by industry; ensure compliance to pertinent and mandatory regimes; reduce stress on inter-departmental management and overheads; improve cybersecurity awareness across an organisation; and promote a framework driven approach that ensures a complete picture of the cybersecurity state.

By improving the level of CSM through CNS Group's Aegis dashboard and consultancy services, IT security teams can finally have the confidence deserved in today's complex threat landscape.

For more information please visit www.cnsgroup.co.uk

TRADITIONAL CYBERSECURITY SPEND COMPARED WITH CYBERSECURITY SPEND ON AEGIS PROGRAMME

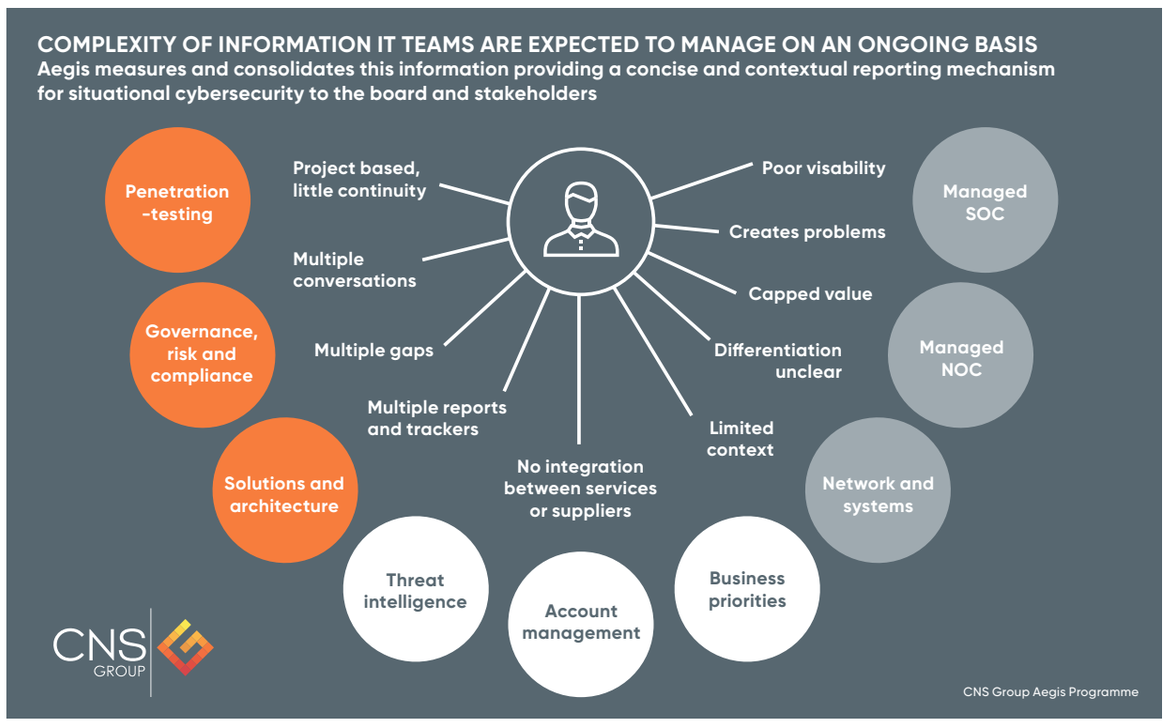
Overview of company's full cybersecurity posture from Aegis provides framework for future spend



CNS Group Aegis Programme

COMPLEXITY OF INFORMATION IT TEAMS ARE EXPECTED TO MANAGE ON AN ONGOING BASIS

Aegis measures and consolidates this information providing a concise and contextual reporting mechanism for situational cybersecurity to the board and stakeholders



CNS Group Aegis Programme

Research was carried out at Infosecurity Europe 2017. Total sample size was 172 IT security professionals. Fieldwork was undertaken June 6-8, 2017. The survey was carried out face to face.

SOCIAL ENGINEERING

Jason Hetherington/Getty Images

Thwarting the tricksters out to get your money

Phishing emails remain the main weapon used by hackers trying to steal valuable information and cash, but there are ways of protecting your business

DAVEY WINDER

Think of social engineering, in the context of information security, and you probably conjure up an image of Nigerian scammers promising millions in return for bank account details plus a small transaction fee. You probably don't think that it might involve the "virtual kidnap" of a loved one.

Michael Levin, formerly deputy director of the National Cybersecurity Division of the US Department of Homeland Security and now chief executive at the Center for Information Security Awareness, recounts how the threat works.

Making full use of intelligence from social networks, as well as the malware compromise of mobile devices, attackers stage a fake kidnapping. A call, possibly spoofed to look like it's coming from the victim's phone, informs you of the hostage-taking and ransom demand. You may hear what could be your partner sobbing or screaming in the background.

This is social engineering at its most evil; the devil literally being in the detail. By hacking into your computer, your phone and your social networks, they know enough to make the threat very convincing indeed. By compromising a smartphone and having access to the GPS location information, the cybercrooks can even convince the victim that they are watching them.

Panic is induced and ransoms are paid. Earlier this year, the FBI arrested one woman allegedly involved in such scams, involving $28,000 in ransoms.

More commonly criminal social engineers will look to employ such intelligence gathering exercises to gain access to corporate networks and the valuable data stored within. The *2017 Verizon Data Breach Investigations Report* shows one in every 14 phishing emails results in a malicious attachment or link being opened, and phishing is now present in one in five security incidents.

What's more, the latest *Enterprise Phishing Resiliency and Defence* report, from social engineering educators PhishMe, reveals such attacks are up 65 per cent from last year. That's worrying as phishing is the de facto tool of social engineering used by cybercriminals to hack humans and gain access to enterprise networks and the valuable data they contain. Some 15 per cent of these emails, according to the PhishMe report, will contain a malicious link and rely on entertainment, social media connections or reward as the emotional encouragement to click through.

So, how can the organisation best ensure that relevant employees are both aware of these threats and enabled to deal with them accordingly? To answer this, we first need to consider who those relevant employees are?

> Employees can become the first line of cyberdefence, able to spot a socially engineered phishing attempt a mile off

Graeme Park, senior consultant at Mason Advisory, says the simple answer is everyone. "It's usually easy enough to elevate a user account to an administrative account or take control of another computer once they have access to the company infrastructure," he says.

But some employees make more attractive targets, according to Mark Crosbie, head of trust and security at Dropbox, who warns that "those with strict business targets can be particularly at risk". Sales staff might be susceptible to being lured with the promise of a business lead, especially as, Mr Crosbie points out, "they often work with external organisations, so giving the attackers added scope to mimic trusted sources".

The C-suite should also look to itself as a potential target. The *iPass Mobile Security Report* suggests C-level executives, including the chief executive, are at the greatest risk of being hacked. This comes as no surprise to Alan Levine, cybersecurity adviser to Wombat Security, who points out that business leaders' digital identities "can be golden keys to valuable personal and professional data".

Stephen Burke, chief executive at Cyber Risk Aware, recalls one chief financial officer (CFO) receiving a fake email supposedly from the chief executive and instructing him to wire money into an account with an explanation promised on his return from a meeting.

"The result was the CFO wired the money and the success of this fraud was down to the fact that the criminals knew the CEO was out of office," says Mr Burke. How did they know? By simply calling the company, using publicly available information from social and corporate media, and establishing the chief executive's agenda for the day on some believable pretence.

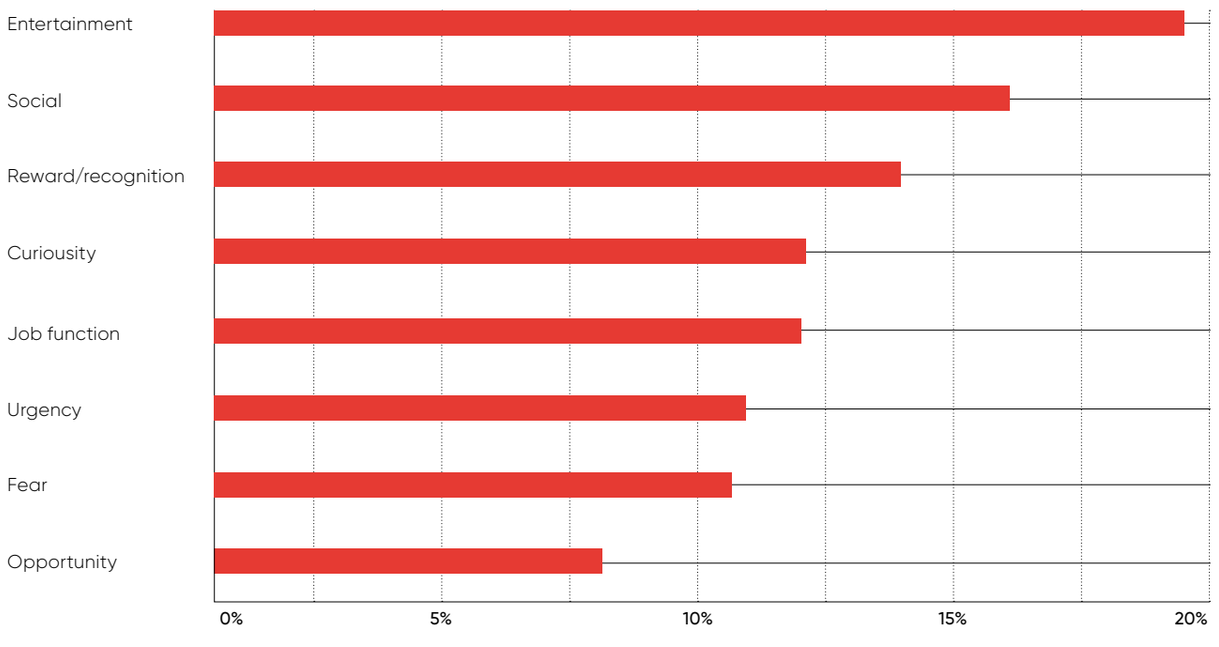
That's not to say that people should be considered the weakest link in security; quite the opposite. Aaron Higbee, co-founder at PhishMe, argues that with effective conditioning techniques in place "employees can become the first line of cyberdefence, able to spot a socially engineered phishing attempt a mile off".

So is awareness training the be all and end all of social engineering defence? "Advising people not to open suspicious emails, click on unexpected attachments or visit unvalidated websites only works if the attachment or email looks suspicious or the website is evidently a spoof," says Amanda Finch, general manager of the Institute of Information Security Professionals. The problem is that the threat actors are getting better at what they do and pulling the right triggers to offset suspicion.

Steven Furnell, professor of IT security at Plymouth University, recommends using the LIST acronym to emphasise core cyber-principles is the best method of achieving this. Legitimacy: should you be asked for this information and would you normally provide it this way? Importance: what is the value of this information and how might it be misused? Source: are you confident that the source of the request is genuine and can you check? Timing: do you have to respond immediately? If in doubt, take time to ask for help.

MOST SUCCESSFUL PHISHING CAMPAIGNS

AVERAGE RESPONSE RATE BY CATEGORY OF PHISHING CAMPAIGN



PhishMe 2017