Cyber security: Non-negotiable basics

Today, organisations are rightly working to ensure their internal networks, data assets and customer - and client-facing websites are well protected and that business continuity and response plans are in place in the event of a cyber attack. The cost of cyber breaches can be ruinous, not only as businesses temporarily go offline, but the long-term reputational impact that comes with the loss of customers' and the public's trust.

The Chartered IIA's Mind the Gap research looks at how cyber risk has been particularly exacerbated by the coronavirus pandemic. Businesses have had to juggle competing priorities and operational disruption whilst ensuring that remote devices and networks are secure. At the same time, criminals have sought to exploit remote working protocols by increasing the pace and sophistication of cyber-attacks.

To help you make sense of this growing risk area is our cyber security report 'Mind the Gap: Cyber security risk in the new normal'. A tool enabling you to provide assurance on cyber security culture within your organisation.

By now all organisations should, at the very least, be certified under the UK government's Cyber Essentials scheme, which encompasses five key technical controls:

- Boundary firewalls and internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management

To achieve the basic-level certification organisations must self-assess their systems and this must then be independently verified. The second level of certification, Cyber Essentials Plus, goes a step further by

requiring that systems are independently tested, and Cyber Essentials is integrated into the organisation's information risk management.

However, the mitigation of cyber security risk means more than simply updating firewalls and malware protections. While critical, such measures alone fail to account for the scope of future risks associated with cyber and technology vulnerabilities. Organisations, through strong governance, risk management and third-line assurance, must work hard to stay on top of this pervasive and rapidly evolving threat. Today's measures may not be enough to defend against tomorrow's cyber risks; therefore, organisations must be as forward-looking as possible on the cyber front.

Cyber culture

The main message of the Chartered IIA's Mind the Gap report is the gap between the work of internal audit in providing assurance on cyber security risk, and assessing and promoting a cyber security culture in the organisations they serve.

Consider your own audit strategy and the assurance provided over the last 18 months.

Does it address culture or focus on specific risks and controls?

If your answer is the latter, then you are not alone. The research found that only a third of chief audit executives reported a direct contribution to an effective
cyber security culture through their organisation's cyber security strategy/policy.

Dedicated cyber resource

All organisations of scale should have established, or be in the process of establishing, a dedicated cyber security function. Whether a sub-team of the existing IT function or a dedicated resource that reports directly to the chief security officer (CSO), companies must be installing a true end-to-end cyber security effort. This resource may be responsible for routine cyber hygiene such as patch management, firewall and malware protection updates, password management, data encryption, penetration testing and so on, but should also have a holistic perspective and review business processes and network system design - and what vulnerabilities these may present.

The organisation must understand how well designed and managed its defences and system processes are and accountability for this should lie with a dedicated resource. From an internal audit perspective, CAEs should be working to understand whether the organisation is appropriately resourced in this regard.

Emerging technology versus organisational strategy

More than that, however, there should be communication between senior management and this resource to ensure there is a clear understanding about the future strategy of the organisation, the extent to which that strategy will depend on technologies and, consequently, what potential vulnerabilities such technologies present.

The UK's National Cyber Security Centre has signalled that future attention will need to be paid to the increasing prevalence of automation and the Internet of Things (IoT), a term used to describe the

interconnectivity of smart devices.

The rise of IoT means the number of exploitable vulnerabilities is escalating. The burgeoning 'fourth industrial revolution' will increasingly see manufacturers and other companies incorporate internet connectivity into their production methods and service delivery to gain efficiencies, increasing the potential for competitors or rogue actors to disrupt production lines and steal sensitive data.

The NHS was one of the more notable victims of the WannaCry attack in May 2017 that exploited a Windows 7 security hole to infect more than 230,000 computers in over 150 countries. Hackers brought down networks and held data hostage, endangering the lives of patients. Given the value of cyber crime, it is unsurprising that early in 2021 allegations surfaced of state sponsored hacking of facilities manufacturing coronavirus vaccines. Findings from the 2021 cyber security breaches report by the UK Government support the need for a cyber culture with only 31% of businesses having a business continuity plan that covers cyber security and less than a quarter with cyber policies that cover home working.

In recent years , medical devices such as pacemakers have become 'smart devices' prone to security flaws like any other device. Yet businesses continue to exploit the potential of automation. Already financial reporting and analytics, online marketing and even anaesthesiology can be carried out by robots, improving profit margins. This trend, however, creates scope for unmanned processes to be hijacked by malicious outsiders.

There is therefore a genuine emerging threat of critical smart devices and automated processes, whether life-saving medical apparatus or self-driving cars, being hacked and putting lives at risk.

CAEs should broach this with the audit committees and consider planning engagements to review the validity and robustness of management thinking around the future strategy of the organisation, what technologies will be required to enable that strategy and what relevant assurances will be necessary in the coming years.

Quantum leaps

It is not only organisations' future use of emerging technical applications that should be considered, but the computing capabilities that may come to underpin such applications. While the development of quantum computing is still in its infancy, some estimate that this next generation of computers could be market-ready within the next ten years. Quantum processors have the potential to process quantities of data on a scale that was not previously possible. It is therefore feasible that the next generation of computers will require a new standard of cryptography to keep internet communications and data assets secure.

Having a cyber resource within the organisation that is familiar with quantum processing may seem like a fanciful idea today. But the pace of innovation is such that we are likely approaching a new era that presents unforeseen security challenges. It is therefore a must that organisations stay abreast of technological developments and their implications for cyber security.

Internal audit has a role to play in evaluating to what extent the cyber function is staying on top of such developments and management/the CSO is factoring into strategic and risk considerations future technological advances that, while currently not a reality, may soon require a radical overhaul to security measures and system design. We would not expect preparedness for leaps in computing power to feature in next year's audit plan. However, the audit committee and chief audit executives may seek to gain an

assurance that the first line of the organisation is thinking sufficiently about future strategic technological threats.

Critical infrastructure

State-sponsored attacks are already here and are due to increase, which has serious implications for operators of critical infrastructure. Knocking out the electrical grid may seem like a dystopian fantasy, but in 2015 a Ukrainian power station was taken offline in a cyberattack that temporarily left a quarter of a million people without electricity.

Legislators are already aware of the cyber security implications for critical infrastructure providers. The UK's Network and Information Systems Regulations 2018, for example, encompasses measures and requirements that apply to "providers of essential services" such as energy, transport, water, health and digital infrastructure.

Consequently, it is not only internal failings and breaches that expose organisations to cyber risk. While essential service providers themselves should be concentrating their efforts to fend off attacks, organisations that *rely* on such services should have contingency measures in place should such critical infrastructure be taken offline.

For this reason, CAEs should be thinking about cyber security beyond the perimeters of the organisation itself and reviewing whether business continuity plans consider major outages at services providers as fundamental as the National Grid, as well as other key suppliers and network hosting services.

It is imperative that boards and internal audit future-proof their thinking around cyber security. Those organisations that dedicate resources to this threat, understand how technology will enable their strategy and vision, and stay on top of the scope of the threat and methods of attack will be more resilient than their peers.

Anjola Adeniyi, managing consultant for IBM, shares his knowledge on cloud security and cognitive security and what you should be looking out for and focusing on.