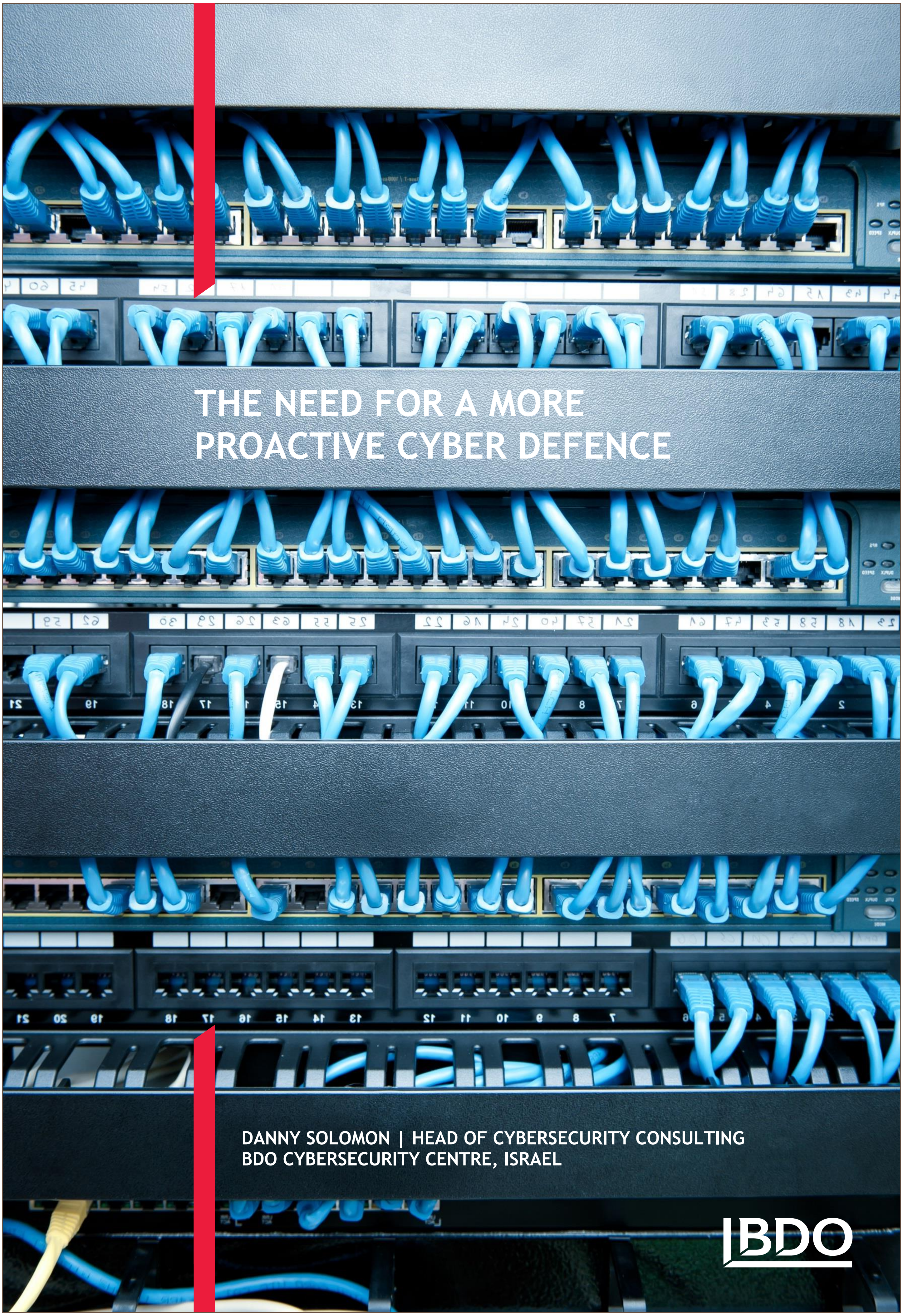

THE NEED FOR A MORE PROACTIVE CYBER DEFENCE

DANNY SOLOMON | HEAD OF CYBERSECURITY CONSULTING
BDO CYBERSECURITY CENTRE, ISRAEL

In the current dynamic security threats landscape, organisations need to prove to stakeholders that they pay more than lip-service to cybersecurity. To do this they need to demonstrate two things: Firstly to 'raise their gaze' and establish better sight or awareness of the threat environment, coupled with greater self-awareness of their own failings and weaknesses. The second is to 'raise their game' - by developing a higher state of readiness to deal with cybersecurity incidents.

But what does this mean? How can organisations justify establishing the capabilities and appropriate level of maturity in their security operations and establishing a proper defensive posture? What capabilities and maturity level do they need in their security operations? Danny Solomon, BDO Israel's Head of International Consulting in the firm’s Cybersecurity Centre, provides some thoughts.

Cyber threats are more potent than most boards recognise, and they prove consistently that static security concepts alone are ineffective in the face of advanced attackers. In the meantime, firms are investing in security technology and discovering that the technology is being persistently undermined by different attack methods.

Most are over-confident in their ability to withstand an attack, or ignorant of the potential causes of their own security failure, and many underestimate the probable long term losses or damage to the organisation and its reputation. This is essentially because management's attitude to securing the organisation’s information and systems is reactive. Even among the more proactive companies, dangerous risk judgments are being made about where to invest in protecting against a breach, and how to invest in recovering from the compromise of systems.

RAISE YOUR GAZE

Organisations need to be informed and prepared for what they might face, and establish the processes and procedures to cope with a severe cyber event. Unfortunately, organisational preparedness tends to build heavily on hindsight or focus on historical threats, irrespective of their evolution.

Similarly, organisational awareness tends to dwell on the more familiar vulnerabilities, often because they have been targeted. Both point to a lack of insight: insight into what is within their threat landscape; insight into what the potential impacts could be on the organisation; and insight into the pace of evolution.

The essence of a pre-emptive approach to security and resilience is based upon developing both insight and foresight, and the adage that being 'forewarned is forearmed' is always the justification for investing in intelligence and preparation as part of an advanced cyber defence strategy. Good management practice and preparedness really requires the ability to anticipate events long before they happen, and to develop a planned response to each scenario. Hence a key element of advanced cyber defence is developing awareness of external and internal factors.

Developing awareness of cyber risk should incorporate the monitoring of relevant intelligence, the mapping of high-risk digital assets, an evaluation of more vulnerable staff, regular security assessments to enable data flow protection analysis and ultimately risk scenario building. This awareness should inform organisational preparedness in helping management to assess their risk posture and define their risk tolerance. More importantly it should prioritise investment in the development and refining of both defensive and response capabilities.

However, more than defining the requirements, the cyclical process for maintaining awareness of the evolving threat landscape should also drive managers to proactively review flaws in their plans and identify barriers to effective performance through regular vulnerability tests and security exercises. The ultimate prerequisite is that defence needs to develop situational awareness to combat the levels of innovation and sophistication that threat actors are introducing.

RAISE YOUR GAME

The shift towards a more resilient posture first requires a more proactive approach to adopting cyber resilience, and a determination to win in the upcoming confrontation with malicious adversaries. But the reality that all companies face is harsh. They are invariably weaker than the opposition, unprepared for the challenge they must meet and quite unaware of the scenarios that underlie the risk.

So it is no surprise that they find it difficult to grasp what an enduring and relevant security model really looks like, let alone what constitutes 'resilience'. There is daily evidence that static security postures are ineffective when faced with an advanced attacker who has the ability to apply a sophisticated approach that corporate security can neither anticipate nor detect in time to effectively prevent. At its core this is what resilience should be.

We should conclude that information security is proving to be a static concept in the way it is being implemented, even as preventative security. The persistent perimeter approach commonly adopted shows the delusion that has plagued security concepts since the building of the Maginot Line. The issue is much less about the nature of the security concept, but more about the 'doctrine' that companies adopt to combat the threats.

Industry needs to move from securing concepts to defending concepts. Defence is a more dynamic concept because it incorporates the assumption that we have to detect and respond to an attack in real time, and we require various options with which to respond, depending on the objectives and methods of the attacker.

This is increasingly the case as organisations are learning that the attack process, from the attacker perspective, from first reconnaissance to full breach attempt can last for days, weeks or even months. In the case of espionage and the evidence of malware like 'flame' or 'the mask': the end game is not assault but the exfiltration of information that can persist for years.

An advanced approach to cyber defence should consider adopting a more proactive defence posture, which needs to be seen as a different doctrinal approach. A cyber defence assumes that technical measures will detect threats and repel attacks. This must be based on relevant threat intelligence, preparation and testing of response measures and maintained as part of a developed detection-response doctrine. It requires a high state of situational awareness based on an effective monitoring and detection capability, and only then can a company establish a response capability to deal with what can reasonably be anticipated.

SO HOW SHOULD ORGANISATIONS TAKE THE FIRST STEP TOWARDS DEVELOPING RESILIENCE?

Preparation of a resilient posture needs overt C-level leadership, because the management of future crises starts now, long before the crisis is apparent. Managers and leaders need to be informed and prepared for what they might face, and failure to prepare is a failure of management to protect the enterprise they are entrusted with.

Invariably the commitment of resources to preparation are only forthcoming when there is clear awareness of the risk, and it is most clearly obvious where a severe breach has already occurred to escalate the issue. Organisations should first focus on developing an awareness of their vulnerabilities that will provide tangible evidence of breach implications, and then test the efficacy of measures they have in place to bring their situation into clear focus and end any complacency and speculation about risk. This will identify the gap in capabilities that they need to fill, and then they have to find the quickest and most cost effective method for filling that gap. In many cases that will require technology like a security information and event management (SIEM), or more human-based security operations (SecOps) functions requiring operators, analysts and responders.

Cyber defence is effective in the majority of cases where it is implemented comprehensively but, for most organisations, the intensity required for such a high level of readiness and awareness is complex and costly to maintain. In recent years the more quick and cost-effective method is to outsource much of the complexity to a Managed Security Service Provider (MSSP). Most companies struggle to justify the resources to retain a full-spectrum cybersecurity team or to maintain up-to-date cybersecurity capabilities.

Organisations are increasingly focusing on their business and turning to outsourced services. A managed service allows companies to focus their attention and resources on the aspects of their internal organisation and processes that sustain a higher state of awareness and readiness.

ABOUT THE AUTHOR

DANNY SOLOMON

HEAD OF CYBERSECURITY CONSULTING
BDO CYBERSECURITY CENTRE, ISRAEL

Danny leads the intra-office liaison at BDO Israel’s cybersecurity centre, supporting BDO partners around the world in positioning advanced cybersecurity and risk services. He has 20 years of experience in professional services consulting and has led more than 300 engagements with some of the largest companies in the Fortune 500 with proprietary concepts in areas of scenario-building, cyber defence, cybersecurity framework development and maturity assessment.

Danny has established programmes for cyber resilience, counter-espionage programmes, and enterprise security risk internationally in banking, high-tech, oil & gas and manufacturing.

He has provided close support to Board-level and C-suite executives, facilitating strategic processes, including: risk assessments, applied threat intelligence, resilience planning, managed security services and incident response capability building. Prior to joining BDO, Danny was Consulting Lead at Cisco Systems Cyber Centre of Excellence.

ABOUT BDO'S GLOBAL CYBERSECURITY LEADERSHIP GROUP

Our corporate methodology incorporates several proprietary models for supporting organisations in developing and improving their resilience posture. From establishing compliance and building towards a proactive approach and through the ongoing development of capabilities, with effective security risk management, we work with our clients to quickly attain higher levels of maturity and resilience.

For more on BDO Global Cybersecurity, visit:
https://www.bdo.global/services/advisory/cybersecurity

GLOBAL CYBERSECURITY LEADERSHIP GROUP:

SHAHRYAR SHAGHAGHI
Technology Advisory Services National Leader,
Head of BDO USA Cybersecurity
+1 212 885 8453
sshaghaghi@bdo.com
Resident Country: USA

GRAHAM CROOCK, CISA, IEEE, AGASA
Director, IT Audit, Risk & Cyber Laboratory
+27826067570 or +27824654539
gcroock@bdo.co.za
Resident Country: South Africa

LEON FOUCHE
Partner and National Cybersecurity Lead
+61 7 3237 5688
leon.fouche@bdo.com.au
Resident Country: Australia

JASON GOTTSCHALK
Partner, Cybersecurity Practice Leader
+44 (0)79 7659 7979
jason.gottschalk@bdo.co.uk
Resident Country: UK

SANDRA KONINGS
Partner, Cybersecurity Practice Leader
+0031 (0) 6 5150 8151
sandra.konings@bdo.nl
Resident Country: Netherlands

ANDREAS VOGT, PH.D.
Director / Head of Section
BDO Security & Emergency Services
+47 48171714
andreas.vogt@bdo.no
Resident Country: Norway

OPHIR ZILBIGER, CISSP, CRISC
Partner, Head of BDO Israel Cybersecurity Centre
+972-52-6755544
ophirz@bdo.co.il
Resident Country: Israel

FOR MORE INFORMATION:

GO MARKETING

Twitter:
@BDOglobal

Email:
marketing@bdo.global

This publication has been carefully prepared by BDO.

‘BDO’, ‘we’, ‘us’, and ‘our’ refer to one or more of BDO International Limited, its network of member firms (‘the BDO network’), and their related entities. BDO International Limited and each of its member firms are legally separate and independent entities and have no liability for another such entity’s acts or omissions. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients. Please see www.bdo.global/about for a more detailed description of BDO International Limited and its member firms. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, the member firms of the BDO network, or any other central entities of the BDO network. BDO is the brand name for the BDO network and for each of the BDO member firms.

This publication contains general information only, and none of BDO International Limited, its member firms, or their related entities is, by means of this publication, rendering professional advice or services. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact a qualified professional adviser at your local BDO member firm to discuss these matters in the context of your particular circumstances. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

Editorial: BDO Global Office, Belgium

www.bdo.global