SWIMMING WITH SHARKS

IDC Analyze the Future

Your Evaluation of Security Maturity and Best Practice against peer organizations

INTRODUCTION

Running your enterprise in the 21st century is akin to swimming with sharks. The danger is clear: threat actors are becoming more potent, more organized and more collaborative by the day. Yet you need to swim in the ocean of Digital Transformation, which is becoming a mission critical concern for today's CEO. However, it also means swimming deeper into the shark infested waters.

Digital transformation technologies – big data/analytics, cloud computing, mobility and social business – take corporate applications and data outside the safety of perimeter controls at the endpoint and the network. This represents a loss of visibility and control for security professionals. Not only are you swimming through murky waters, but the door to that shark-proof cage that used to protect you has swung open!

Avoiding digital transformation is not an option. One need only consider the fate of enterprises such as Blockbusters and Borders that have failed to adapt to the new reality to understand the implications. Instead, a step change in both technological approach and strategic mindset are required. This report aims to uncover best practice exhibited by your peers with the most mature approach towards security. In order to swim with the sharks, and maybe even bite back, a new outlook is required.

USING THIS REPORT

This report aims to provide you with insights into the characteristics and progression of maturity in security. It identifies examples of best practice that you can aspire to in order to improve your security maturity. It also highlights innovation accelerators that have a particularly strong impact on boosting maturity levels. Finally, it offers recommendations for how you can improve your position in comparison with your peers. These insights emerge from a survey of 500 senior security decision-makers based in France, Germany, Italy, Spain and the UK.

YOUR PEERS' MATURITY PROFILE

Based on our survey of 500 senior security decision-makers, IDC has broken the market down into five categories of maturity. From low to high, these are:

ad-hoc
opportunistic
repeatable
managed
optimized.

Enterprises are typically distributed into a classic 'bell curve' as shown in figure 1:

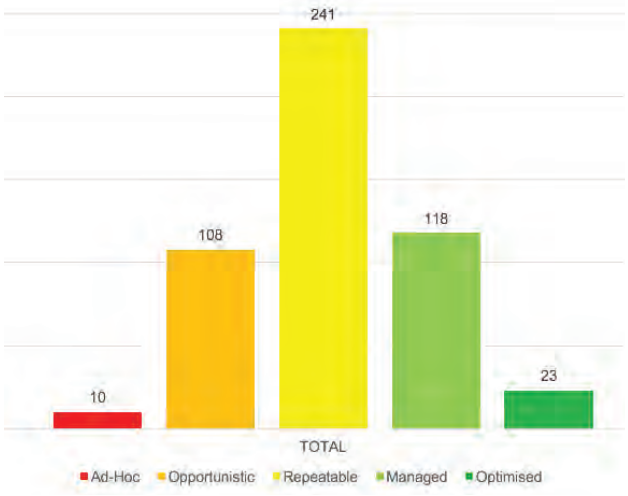

Figure 1

Source: IDC, 2016

There are very few of your peer organizations at the low end in their approach towards security, and also few at the top end. Instead, the majority of peer enterprises sit somewhere in the middle. If you aim to swim with sharks without getting bitten, you should aspire beyond parity of your peers and embrace best practice. The next section of this report gives indication of what best practice in security looks like.

SECURITY BEST PRACTICE

Traditionally, security technology has aimed to protect enterprises from known threats. By gathering devices, applications and data behind the safety net of the firewall, perimeter controls at the device and network levels could keep those known threats at bay. However, such preventative security models are being rendered insufficient as a stand-alone approach by two trends:

- Digital transformation is taking corporate applications and data beyond the perimeter, and outside the visibility and control of in-house security teams.
- The sheer scale of threats is unprecedented. The number of new malware variants emerging on a daily basis is over a million. It is simply impossible to generate signatures at a rapid enough pace to maintain traditional defenses that aim to block new threats.

Quite clearly, new approaches are required that will help enterprises to identify and respond to unknown threats as well as blocking out known threats. Security must become proactive, seeking potential indicators of compromise to remediate rather than waiting for an attack to become evident. However, this requires a mental leap in security strategy. An analysis of what is considered to be limiting security effectiveness across the maturity levels is enlightening, as shown in figure 2 below:

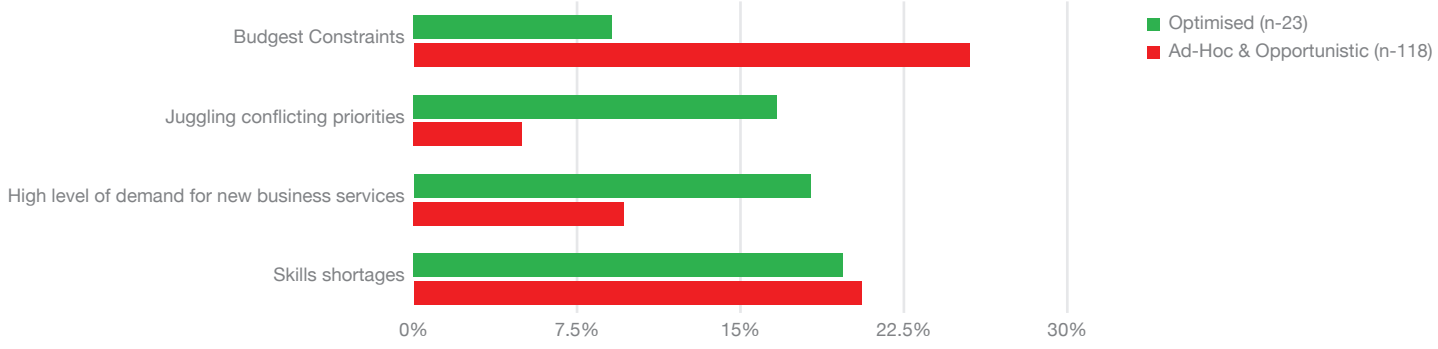

Figure 2

Source: IDC, 2016

There are certain common themes that apply across all maturity levels. Specifically, cost and skills availability are the primary limitations. This is no surprise given the global skills shortage that endures within the security market. However, it is the degree to which further concerns are considered where an insight into best practice emerges.

For lower level maturities, cost pressures and skills shortages are the overwhelming concerns. But at more mature levels, there is a greater balance between these areas and areas such as the management of conflicting priorities and supporting demand for new business services. This highlights a key step change in mentality: best practice in security is to consider the needs of the business.

Once this mental leap has been made, enterprises must consider what this means in terms of practical security approaches. In particular, the progression away from reactive security models towards proactive security is required. In fact, as shown in figure 3 below, there are two clear trends across maturity techniques. The more mature an enterprise is, the less likely it is to not be using proactive security techniques, and more likely to either be planning or already using them.

Proactive Security Adoption by Maturity Level

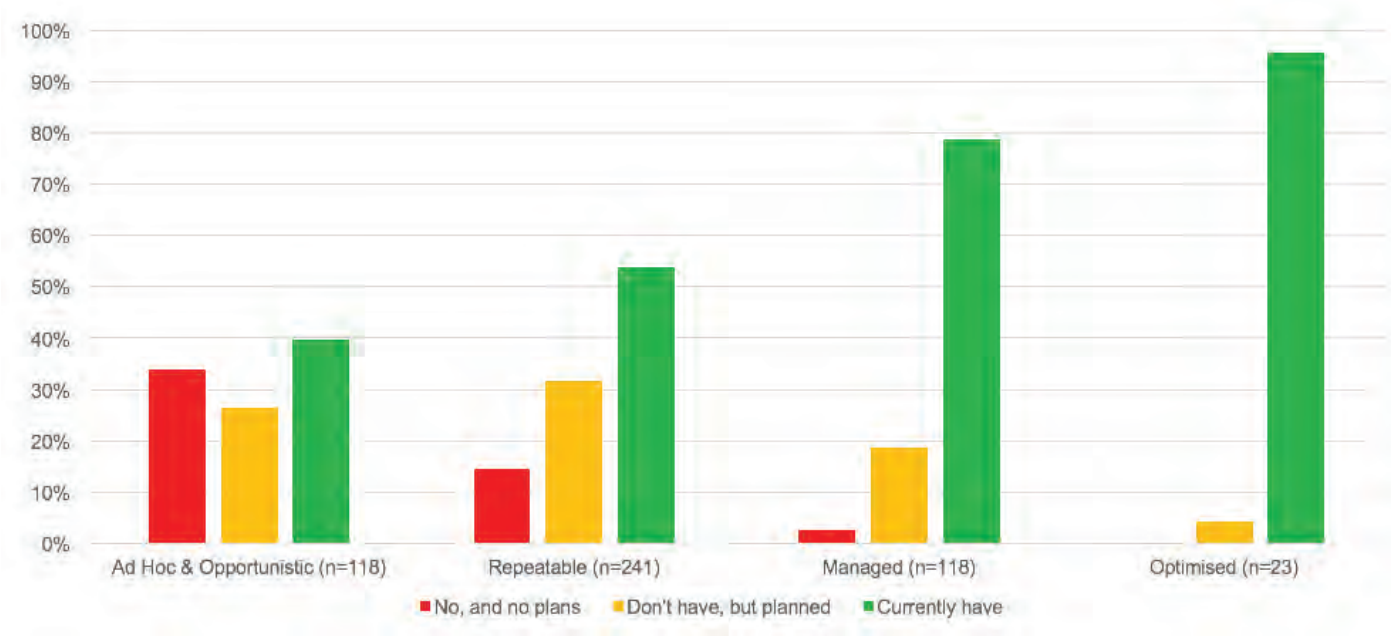

Figure 3

Source: IDC, 2016

According to our survey, key security technologies that enterprises can adopt in order to facilitate these more proactive approaches include threat intelligence, artificial intelligence and heuristic analysis of user behavior. As with proactive technologies, the more mature an enterprise's security approach is, the more likely it is to make use of solutions such as AI and heuristics.

Although proactive security approaches represent an opportunity to move up the security maturity scale, they also bring their own challenges. For example, proactive techniques require the gathering and monitoring of operational and behavioral logs on a far larger scale. Given the pressures on both financial resources that security teams are facing, a grown up discussion of techniques to help lighten the load on internal resources is required. Best practice indicates that there are two potential outlets.

OUTSOURCING

Although enterprise security is tough, the over-riding tendency is to keep control of it internally. There are a number of motivating factors here. For starters, security is viewed as a mission-critical activity and any externalization threatens to reduce the visibility and control that in-house teams hold over their security posture. Managed security services providers (MSSPs) have made great promises in the past, but the reality has not always lived up to that promise. Finally, turning to third parties may even be seen as an admission of failure by in-house teams, acknowledging that cannot do the job alone.

However, in a connected world, no single enterprise stands alone and immune to the threat. This is especially the case when European enterprises possess limited security resources, and where third parties are increasingly well-positioned to provide support thanks to, for example: global scale, industrialized delivery models, better access to skilled personnel, etc. Therefore, for those who aspire to best practice in security, MSS is an important consideration.

Although MSS can be a crutch for enterprises to ease pressures on internal resources, it cannot become the only answer. IDC's research indicates that, rather than wall-to-wall outsourcing, best practice is to find a balance between in-house delivery and MSS that meets both the business goals and the risk appetite of the enterprise. The retention of in—house capability within security operations is important to understand the strategic impact of business decisions on security – and vice-versa. With security increasingly driven on a risk-management basis and as an organization-wide concern, this is a vital characteristic of best practice for business management, let alone security practice.

AUTOMATION

Alongside MSS, another key lever for enterprises to pull in the face of pressure on resources and the imbalance between digital transformation and the evolving threat landscape is automation. Automation allows the management and even delivery of security operations to be handled through technology products. The involvement of in-house personnel helps to retain visibility and control over security.

This will have ramifications for the emergence of AI and cognitive computing within security, which aim to further release pressure on resources by pushing decision-making to machines. However, it is clear that best practice (at least for the time being) will be to retain a degree of human oversight to ensure the smooth running of the machines, or to take the most critical decisions out of robotic hands.