



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:

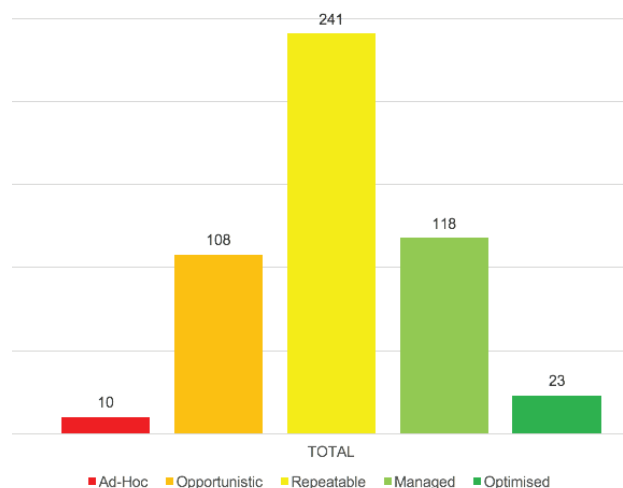


Figure 1

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:

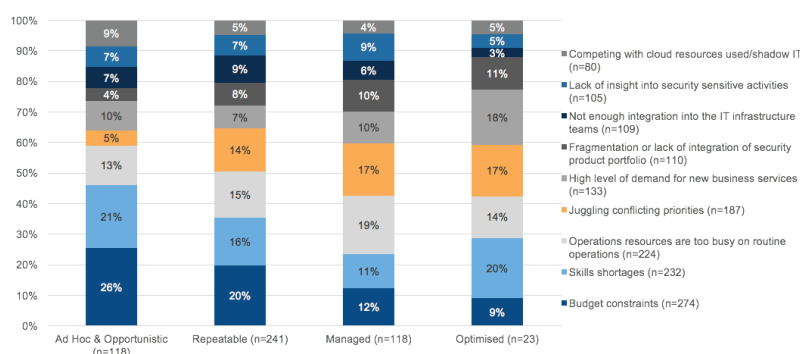


Figure 2

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

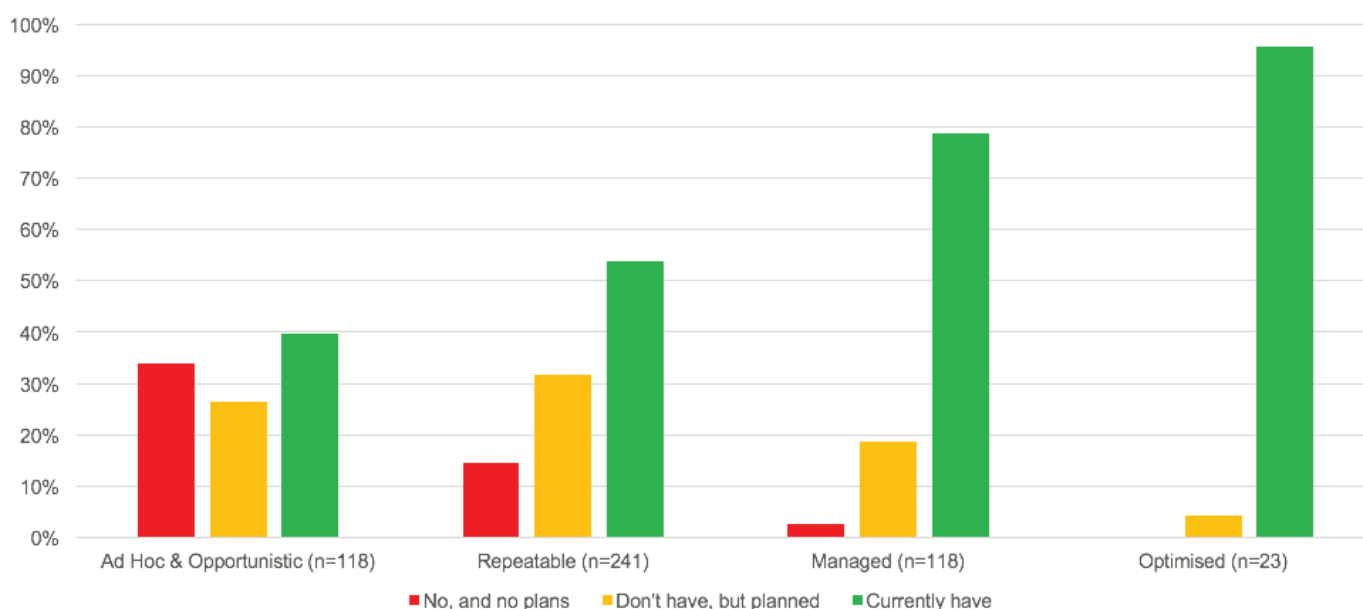


Figure 3

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.

TOLERANCE FOR CHANGE

A final factor to consider in understanding how well firms embrace the need to swim with sharks is their ability to cope with IT change. As outlined earlier in this report, best practice approaches towards cybersecurity represent a deviation from standard behavior that has evolved over a period of decades. In order to enact changes in mentality and philosophy towards security, the ability to embrace change in the underpinning IT is an important enabling factor.

A key example here is digital transformation, which is one of the key reasons why enterprises are being forced to swim in these shark-infested waters in the first place. Standard practice among security professionals may be to seek to block the adoption of technologies such as social business, mobility big data/analytics and cloud. Their adoption represents an exposure to risk. However, this is not the mature approach; instead of blocking digital transformation, the enlightened enterprise must seek to empower users, providing them with the tools to adopt digital transformation securely.

As demonstrated in figure 4 below, the more mature an organization is as defined by this study's framework, the more comfortable they are in coping with IT change. At the low end of the scale, the least mature enterprises tend to struggle with any IT change, or least they struggle when asked to enact anything other than basic changes to applications and services. However, as we move up the maturity framework, it becomes more likely that an enterprise will describe itself as being able to cope with these changes, or even 'very good' at delivery of them.

These findings show that, in today's security environment, one of the keys to being a successful, dynamic enterprise is to take a mature approach towards security and is able to harness (rather than fear) IT change. The door swings both ways, with one theme being a reflection of the other. The ability to make IT changes requires affirm grasp of the security implications. At the same time, in order to adopt a mature stance towards security, an ability to enact the required changes to IT is critical.

Capability for Coping with Change by Cyber Risk Maturity Levels

Q2. When it comes to business requests for new or enhanced applications or services, which statement best reflects your IT department's capabilities?

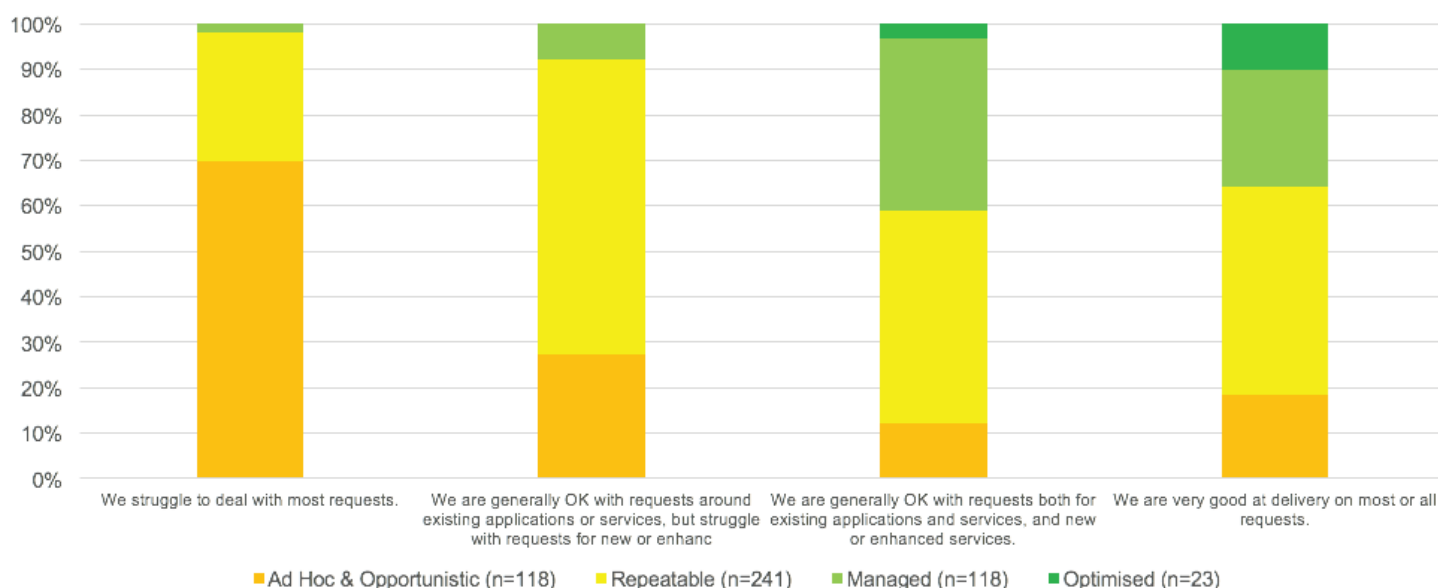
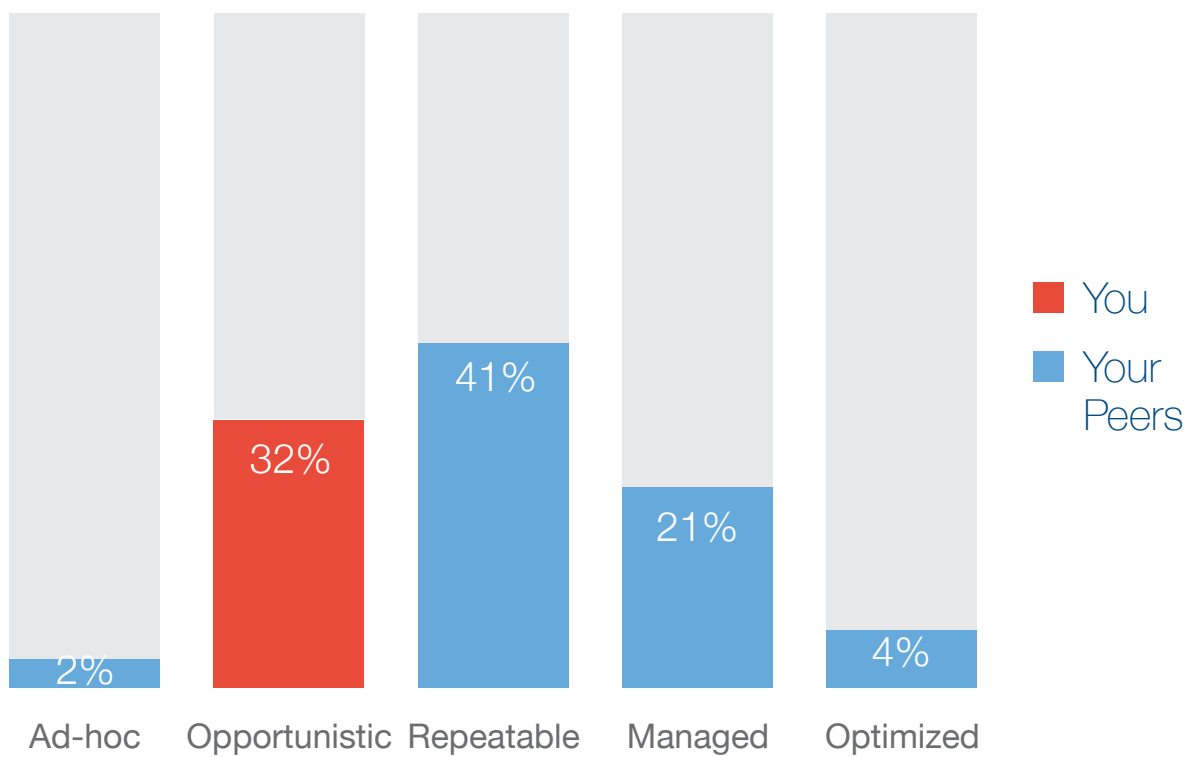


Figure 4 Source: IDC, 2016

CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING

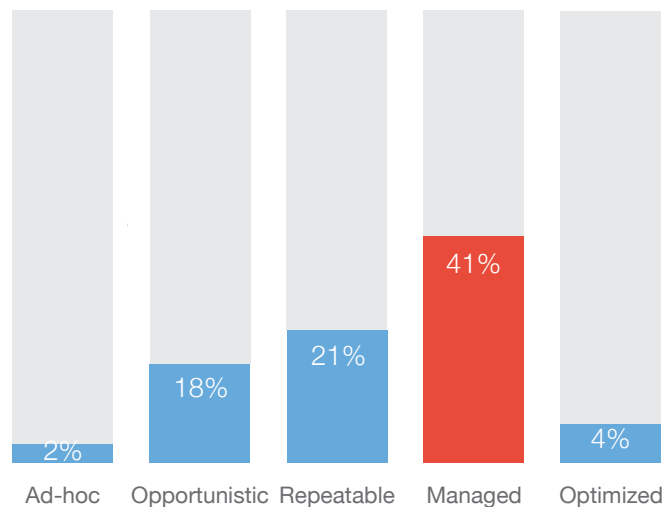
How you compare overall



Thank you for completing the IDC Cyber Risk Assessment. Based on your responses, your readiness ranking is **Opportunistic**, which is second lowest rank of the five different readiness levels.

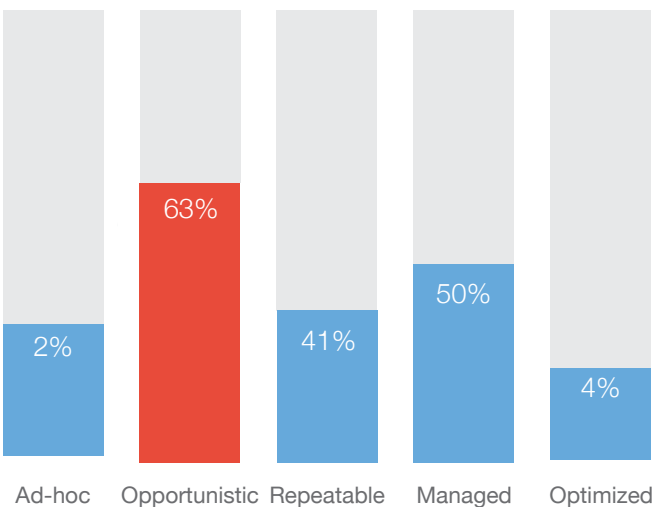
You are in the lowest 20% of companies in the ranking, and have a lot of areas in which to improve. Your business and data are at risk if you do not take urgent steps to improve. You are left open to industry and regulatory sanctions and fines if a breach results in the loss of personal or confidential information.

Your comparison to others in your country



France

Your comparison to companies of similar size



2000-3000



PERFORMANCE RANKING BY CATEGORY

We're now going to look at how you performed in three key areas of Cyber Risk Readiness. In each case, we'll look at how you compared to others in the same readiness ranking of Opportunistic as yourself. To do this, we look at whether you are behind, in-line or ahead of your peers.

If you are in-line, you are broadly comparable to most companies at your level of readiness. If you are ahead, you are doing well in this area and should be looking at other areas to improve to get a balanced approach. If you are behind, you need to focus attention and investment in this area to bring your Cyber Risk Readiness in to line.

If you achieve a rating of in-line or ahead in all sections, you are ready to be moving up a readiness level in short order.

Cyber Risk Management and the Business



Top job! You are ahead of your peers when it comes to managing Cyber Risk in conjunction with the business. You are performing very well in this area of Cyber Risk management but should not become complacent and continually reassess what you do.

Cyber Risk Management Operations and Defence



Warning! You are behind in this core area of Cyber Risk management, and need to urgently improve matters to reduce your exposure to cyber threats and potential fines or loss of reputation.

Cyber Risk Management Breach Detection and Remediation



Job well done! You are performing in-line in this area of Cyber Risk management, but should still look to new approaches to help you improve your overall Cyber Risk readiness.

SECURITY AND THE BUSINESS PERFORMANCE RANKING BY QUESTION

Q1. How does Senior Business Management tend to view the role of IT? (Choose one)

A1: **An enabler of business efficiency**



In your overall level of OPPORTUNISTIC, you are positioned as **INLINE**

When compared with the next level, REPEATABLE, you would be positioned as **BEHIND**

Your approach to risk at the business level is in broadly in line with your peers, showing caution towards risk but taking advantage of them where there is a clear business benefit. However, there is room for improvement here. Leading-edge firms are able to actively identify and manage risks in order to help the business develop. Try to Take a more active role in identifying, analysing and managing risk, while developing a firm understanding of your business' appetite for risk. In this way, a clear grasp can be achieved of where compromise can be achieved where it is in the business' best interest.

Q2. When it comes to business requests for new or enhanced applications or services, which statement best reflects your IT department's capabilities?

A2: **We are very good at delivery on most or all requests.**



In your overall level of Opportunistic, you are positioned as **AHEAD**

When compared with the next level, Repeatable, you would be positioned as **INLINE**

You are ahead of your peer group when it comes to delivering news applications and services quickly and with confidence. While much of your focus on improving Cyber Risk Management can be elsewhere, you should continue to adopt and optimise advanced capabilities around policy, management and automation & orchestration.

Q3. Which statement best describes your attitude to risk at a business level? (Choose 1)

A3: **We are wary of risks, but will take them where we can see a clear business benefit.**



In your overall level of Opportunistic, you are positioned as **AHEAD**

When compared with the next level, Repeatable, you would be positioned as **AHEAD**

Your approach to risk management at the business level is in advance of your peers. You take an active approach in identifying and managing risks in order to help the business develop. However, in order to be truly leading edge you must continue to push the boundaries. Work to establish where compromises can be made, bearing in mind the 'crown jewels' that must absolutely remain locked down at all costs, in order to find new opportunities for development.

Q4. Which of the following do you have in place already to protect your business in the event of an incident? (1-Currently have, 2-Don't have, but planned, 3- No, and no plans)



In your overall level of Opportunistic, you are positioned as **AHEAD**

When compared with the next level, Repeatable, you would be positioned as **INLINE**

A4: a: A formal risk assessment

☒ **No, and no plans**

b: Proactive detection

☒ **Currently have**

c: Response Plan

☐ **Don't have, but planned**

d: Internal communications plane

☒ **Currently have**

e: External communications and public relations plan

☒ **Currently have**

f: Breach notification plan

☐ **Don't have, but planned**

g: Breach remediation plan

☒ **Currently have**

h: Cyber risk insurance

☒ **Currently have**

You are ahead of your peers in how you manage the risk of security breaches and plan your responses in the event of a breach. You are likely armed with a breach response plan that provides guidance of when to begin each stage of the response process, notifying the relevant parties (internal and external) at the appropriate point, and taking steps to remediate the problem. However, as a next step, consider how cyber risk insurance can be harnessed not only to mitigate the potential costs of a breach, but also as a driver for excellence - and thus it becomes a potential source of competitive advantage in how customer data is handled.

10 RECOMMENDATIONS FOR YOUR ORGANIZATION

Here are ten recommendations that provide a framework for your enterprise to improve its level of maturity in security:

- **Compare your position with your immediate peers in terms of industry, size and geography.**
- **Establish your appetite for maturity and where you aspire to be.**
- **Establish the gaps in your current security approach compared to your aspirational state.**
- **Consider making use of third party security specialists to help design and implement the changes required to reach your goal.**
- **Identify the security processes and activities that are critical compared with those that are low value and repetitive.**
- **Consider where lower value activities can be automated to reduce resources.**
- **Consider where outcomes could be improved by working with MSSPs. Lower-value activities may be a good place to start, taking advantage of global and industrialized delivery models.**

However, as MSSP becomes business as usual, consider where specialist capabilities are available that may boost the desired outcomes, which may include cost as well as quality.

Take a risk-based approach towards security that encompasses the whole of the enterprise, All users are a potential 'insider threat', so security culture and strategy must be holistic.

Embed security representatives within new business initiatives from the start. Ensuring that new initiatives are 'secure by design' will make life easier further down the line.