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:

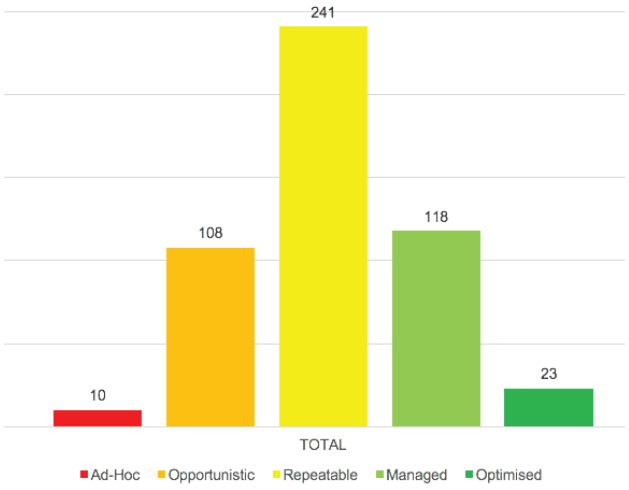


Figure 1

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:

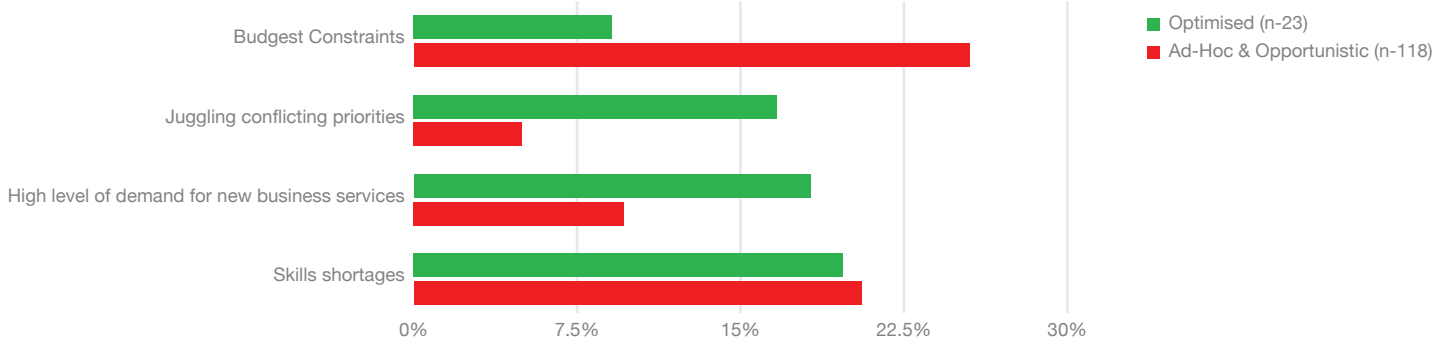


Figure 2

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

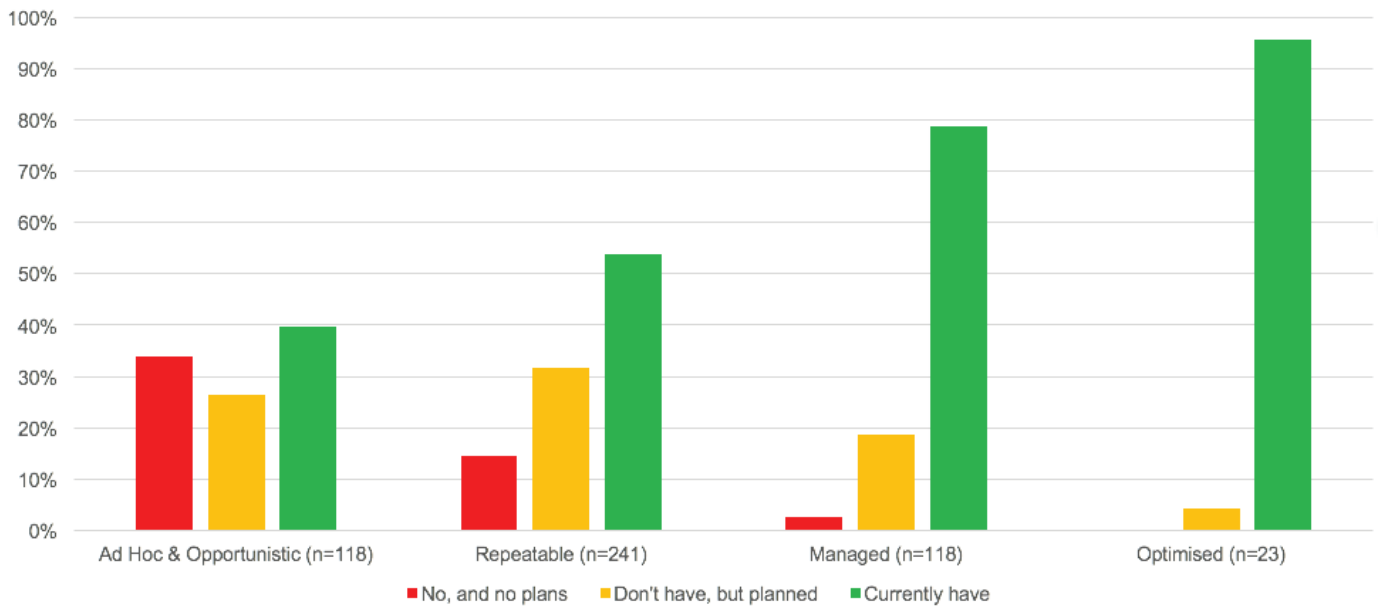


Figure 3

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.

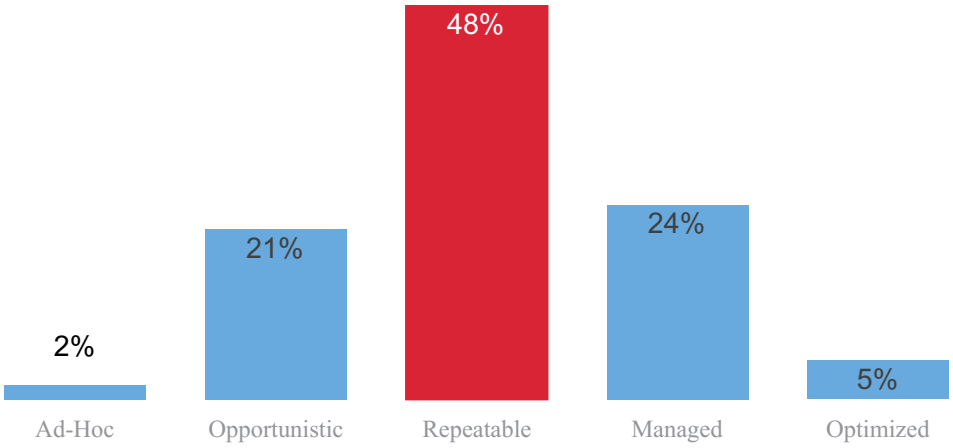
AUTOMATION

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.

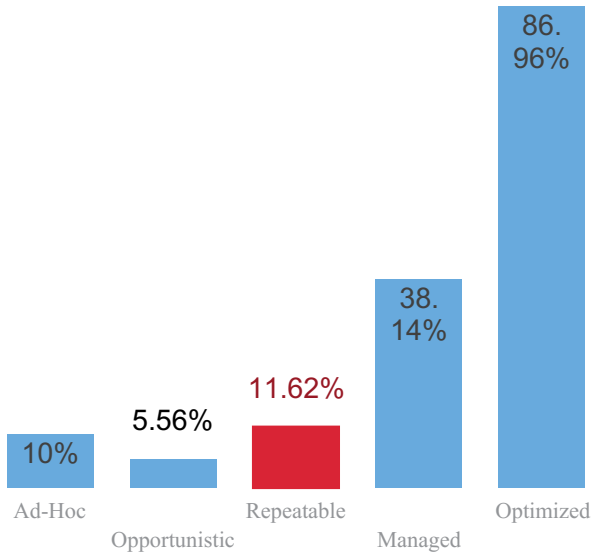
This will have ramifications for the emergence of AI and cognitive computing within security, which aim to further release pressure on resources by pushing decision-making to machines. However, it is clear that best practice (at least for the time being) will be to retain a degree of human oversight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

CUSTOM REPORT SUMMARY AND OVERALL PERFORMANCE RANKING

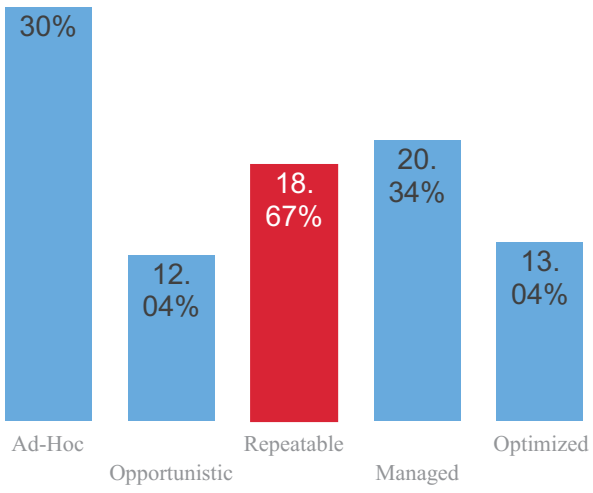
How you compare overall

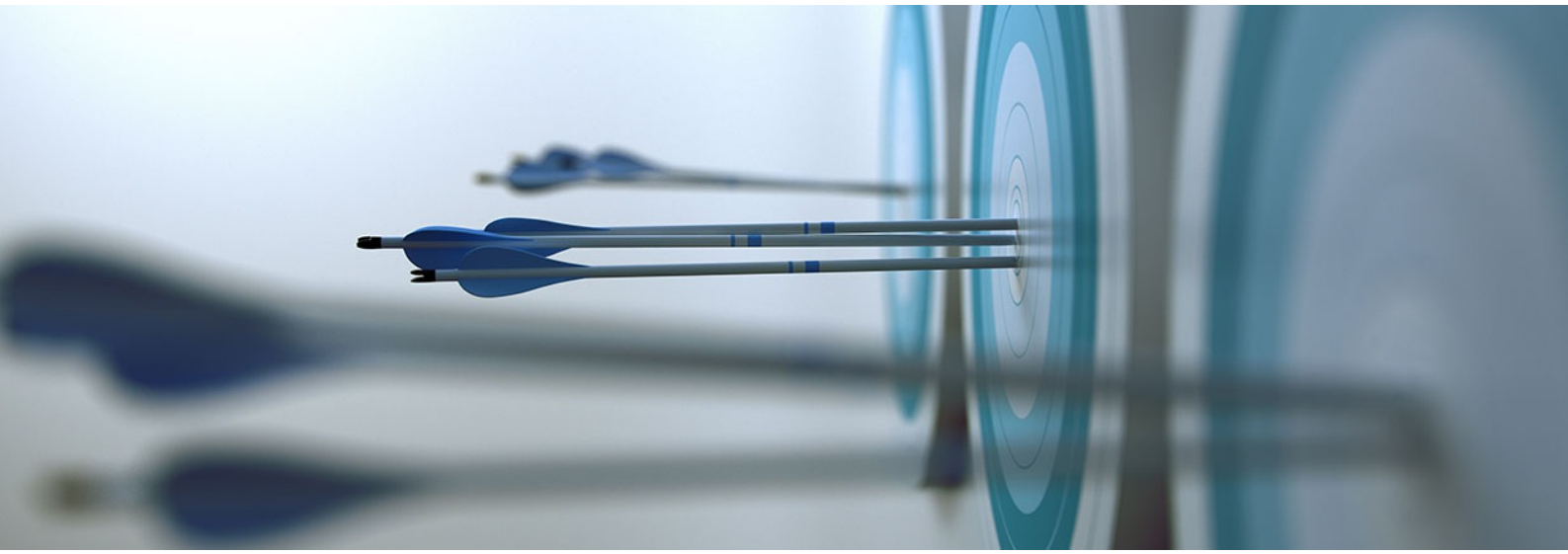


Your comparison to others in your country



Your comparison to companies of similar size





PERFORMANCE RANKING BY CATEGORY

Cyber Risk Management and the Business

Ranking: MANAGED

Impressive showing! You are in-line in this core area of Cyber Risk management,, but should still look to emerging ways to improve your ability to secure your IT domain.

Cyber Risk Management Operations and Defence

Ranking: REPEATABLE

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.

Cyber Risk Management Breach Detection and Remediation

Ranking: OPPORTUNISTIC

Good performance! You are in-line with your peers when it comes to managing Cyber Risk in conjunction with the business. You should still look to form a closer relationship with the business to improve your overall Cyber Risk readiness if you want to move up the readiness rankings.

CYBER RISK MANAGEMENT AND THE BUSINESS PERFORMANCE RANKING BY QUESTION

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 **Repeatable** 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."

Q1: How does senior business management tend to view the role of IT? Please select one

A: An enabler of business efficiency

When compared with the next level, **Optimized** you would be positioned as **Behind**

You should look to ways to improve the awareness and understanding among business leaders of what IT can do to improve the profitability and competitiveness of the company.

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

A: We are generally OK with requests around existing applications or services, but struggle with requests for new or enhance

When compared with the next level, **Optimized** you would be positioned as **Behind**

Look to new ways to deploy and manage IT, through approaches such as automation and risk management, to deliver new services quickly and with confidence.

Q3: Which statement best describes your attitude to risk at a business level? Please select one

A: We will take on risk readily to help the business develop.

When compared with the next level, **Optimized** you would be positioned as **Inline**

Your are performing well, but there is room for improvement. 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.

Q4: Which of the following do you already have in place to protect your business in the event of an incident?

A:

- A formal risk assessment — Don't have, but planned
- Proactive detection — No, and no plans
- Response plan — Currently have
- Internal communications plan — Currently have
- External communications and public relations plan — Currently have
- Breach notification plan — Currently have
- Breach remediation plan — Currently have
- Cyber risk insurance — Currently have

When compared with the next level, **stage5** you would be positioned as **Inline**

You are forward thinking in how you manage the risk of security breaches and plan your responses in the event of a breach. 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.

Q5: Which statement best describes how cyber risk management is handled in your company? Please select one

A: It is typically delegated to IT.

When compared with the next level, **Optimized** you would be positioned as **Behind**

Consider the business imperative for digital transformation and the exposure to risk that arises as a result, consider how IT and the business can work together in order to develop an approach to cyber risk that is appropriate for all parties and can help the business to meet its targets.

Q6: Of the following, who are part of your cyber risk assessment structure?

A:

CEO No	CFO No	COO Yes
Non-executive board-level risk/compliance/security focused member Yes	Executive board-level risk/compliance/security focused member Yes	Dedicated risk/compliance/security role (non-board) Yes

When compared with the next level, **stage5** you would be positioned as **Ahead**

In order to take this framework to the next level, consider how specialists in the fields of risk, compliance and security both in the board room and below it can make a positive contribution to this process. Make effective use of third parties to gauge best practice.

Q7: How early is IT security usually brought into business projects and initiatives? Please select one

A: At the beginning of implementation

When compared with the next level, **Optimized** you would be positioned as **Behind**

Security is unlikely to be involved any sooner than the implementation stage of the project (by which point it will be no more than a bolt-on concern, with variable success) or possibly only when something goes wrong (by which stage it is far too late). Consider how security can play a role at least in the planning stage of any new business initiative, if not sooner.

Q8: How would you describe the level of IT security investment in your organization? Please select one

A: Readily available across the board with a good business case, even for experimental development

When compared with the next level, **Optimized** you would be positioned as **Inline**

In order to strive for further improvement, position security investment as the enabler that is driving the enterprise to achieve business goals and supporting growth in both revenue and profitability.

CYBER RISK MANAGEMENT OPERATIONS AND DEFENCE PERFORMANCE RANKING BY QUESTION

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 **Repeatable** 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."

Q9: To what level do you have the following in place for managing your IT physical security?

A:

- Security staff screening: 3
- Prebooked appointments: 4
- Identity verification: 5
- Man-traps to enter/exit: 1
- Biometric authentication: 1
- CCTV monitoring: 1
- Man-shadowing (staff and visitors must work in pairs or be accompanied): 5
- Change authorization, approval, and logging: 5

When compared with the next level, **stage4** you would be positioned as **Behind**

Approaches such as entry/exit 'man-traps' and man-shadowing ought to become standard practice, and then start looking to more forward-looking techniques such as biometric authentication.

Q10: Which of the following best describes your adoption and implementation of IT security best practice? Please select one

A: We do this on a formal basis (using standards) using our general skills.

When compared with the next level, **Managed** you would be positioned as **Behind**

This is a formal process that leverages expert skills. In order to push this process towards more advanced levels, consider how external expert assessors could be engaged in order to bring an independent understanding of what is best practice given the context of your organisation.

Q11: How prepared are you for the following aspects of your assessment and implementation of GDPR (General Data Protection Regulation) compliance?

A:

- Knowledge of obligations: 4
- Assessment of capabilities and gaps: 1
- Implementation planning: 1
- Implementation execution: 3
- Continuous improvement/best practice beyond the GDPR itself (beyond the regulations): 4
- Understanding mitigation of penalties based on early detection/remediation: 4

When compared with the next level, **stage4** you would be positioned as **Behind**

In order to move up the maturity scale, develop an understanding of the obligations that GDPR brings, plan for implementation of those responsibilities and then execute on that plan.

Q12: Do you tend to invest tactically (point products/as needed) or strategically (part of a plan) in IT security products or solutions? Please select one

A: We mostly buy tactically as issues arise but have some strategic purchasing.

When compared with the next level, **Managed** you would be positioned as **Behind**

Best practice Cyber Risk Management focuses on frequent or real-time reporting. Work on improving you logging capabilties alongside analytics to move from a reactive to proactive approach.

Q13: How often do you report on IT security status to the business? Please select one

A: Weekly

When compared with the next level, **Managed** you would be positioned as **Ahead**

In order to strive for improvement, consider how continuous reporting can act as more than a mere dashboard, but become a driver of business-level decision-making through an integrated operations capability.

Q14: What is your primary means of managing your IT security infrastructure? Please select one

A: We use a combination of specialized management tools with some 'out-of-the-box' tools.

When compared with the next level, **Managed** you would be positioned as **Behind**

It is impossible to secure that which you cannot manage. Best practice is to use integrated tool sets and automation to ensure that policy is applied consistently.

Q15: To what level have you adopted automation in your IT security management? Please select one

A: A good balance of automation and manual processes

When compared with the next level, **Managed** you would be positioned as **Inline**

Best Cyber Risk Managment practive uses automation extensively. Consider areas that would benefit from automation (particularly those that are low-value and repetitive, but also those where speed of reaction is most critical) to achieve a good balance between automation where possible and manual processes where required.

Q16: When it comes to your use of automation, how do you intend to change your use of this? Please select one

A: Stay the same

When compared with the next level, **Managed** you would be positioned as **Inline**

Best practice in Cyber Risk Management is looking to increase automation. Consider how the use of automation can be increased in order to boost the efficiency and effectiveness of your IT security operations.

Q17: Do you make use of the following regarding IT security?

A:

- NGFW (next-generation firewall)
  No
- IPS/IDS (intrusion detection/protection)
  No
- Vulnerability management
  Yes
- Micro segmentation (fine-grained separation and isolation of traffic between specified hosts or domains)
  Yes
- Unified security management (data and information interchange between devices and tools),
  No
- Third-party professional security service (pre-sales/design/implementation)
  Yes

When compared with the next level, **stage4** you would be positioned as **Behind**

The most advanced at Cyber RIsk Mangement make extensive use of a range of security products that are available to offer protection across the corporate network. Working with third party MSSPs to help you design and implement appropriate approaches can also but time to implementation and boost capabilities.

Q25: Which statement describes the extent of your use of managed security services providers? Please select one

A: We use them in a limited fashion, but prefer to do things in-house.

When compared with the next level, **Managed** you would be positioned as **Behind**

In order move in line with the level of standard practice set by your peer group, consider where the use of MSSPs may be additive in order to achieve a position whereby a balance is struck between in-house operations where necessary and the use of MSSPs elsewhere.

CYBER RISK MANAGEMENT BREACH DETECTION AND REMEDIATION PERFORMANCE RANKING BY QUESTION

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 **Repeatable** 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."

Q18: Do you make use of the following regarding IT Security: Breach detection
A:

- Threat intelligence services: No
- Real-time analytics: No
- Advanced threat protection/sandboxing: No
- AI/heuristics: Yes
- Malware scanning: Yes

When compared with the next level, **stage3** you would be positioned as **Behind**

Compliance and best practice means that malware scanning and ATP/sandboxing are now standard technologies and you should examine their capabilities if not already doing so. Analytics and threat intelligence services offer advanced protection against new threat sources, so consider whether these technologies would help, relative to your organisation's risk profile. Artifical intelligence and heuristics are mainly for mature and advanced security operations, so keep these in mind for future reference.

Q19: Do you make use of the following regarding IT Security: Breach response
A:

- Honeypot/intelligence gathering: No
- Forensic logging and analysis: Yes
- Failover/system recovery: No
- Tiger/go teams: No
- External incident response partner: Yes

When compared with the next level, **stage3** you would be positioned as **Behind**

Forensic logging & analysis, and Failover/system recovery are standard technologies and you should implement these if not already doing so. Most larger firms (and many not so large) are now using external incident response services partners, either on retainer or as ad hoc providers, so consider whether this would help reduce your organisation's risk profile. Honeypot/intelligence gathering and Tiger teams are mainly for large, mature and advanced security operations, so these would be later steps.

Q20: Do you make use of the following regarding IT Security: Breach response
A:

- Automated remediation (machine learning based): No
- Policy updates: No
- Disaster recovery policy: Yes
- External disaster recovery providers: Yes
- Compromise assessments: Yes

When compared with the next level, **stage3** you would be positioned as **Behind**

Policy updates and a Disaster recovery policy are standard and you should implement these if not already doing so. Most firms conduct Compromise assessments, and many use external disaster recovery providers, so consider whether these would help improve your DR capabilities. Machine learning-based automated remediation capabilities are quickly maturing, and worth keeping an eye on.

Q21: Have you done the following in regards to understanding your Cyber risk profile?
A:

- Assessed your risk of suffering a cyber breach
  No
- Understand potential scale of exposure
  No
- Done a data assessment of critical data
  Yes
- Understand posture of extended supply chain or partners
  Yes
- Developed a security breach response plan
  Yes

When compared with the next level, **stage3** you would be positioned as **Behind**

We live in an era of inevitable breaches, so it is essential to have a strong idea of the likely impact of such a breach and develop a security breach response plan. This includes understanding the potential scale of exposure and assessing the risk attached to specific data categories, such as personal data. Understanding the posture of your extended supply chain or partners is also essential, both in terms of inheriting security vulnerabilities from third parties, and from the new joint liability rules introduced by GDPR.

Q23: How often do you test your IT security defense capabilities through third-party verification? Please select one
A: Every few years
When compared with the next level, **Repeatable** you would be positioned as **Behind**

These days it's essential that third party validation of security is undertaken, even in advanced environments where 'marking your own homework' can lead to complacency. Continuous validation is now the expected standard, though much of this can now be automated. Services-based penetration tests should be conducted at least every six months, because the threat landscape is changing so quickly. Testing less frequently is putting your organisation at greater risk.

Q24: How often do you test your cyber breach incident response plans? Please select one
A: Every year
When compared with the next level, **Repeatable** you would be positioned as **Behind**

The recommended frequency is between one and three months, depending on the complexity and context of your environment and the threat risk for your particular industry. Leave it longer and you risk key individuals being under-prepared for the inevitable breach, while new legislation may open you up to the risk of significant fines. Aim to improve your testing and reporting, but don't try to target frequency at the cost of capability. Weekly or continuous testing is usually only for the most advanced - or high risk - organisations, where poor incident response would be catastrophic.

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?

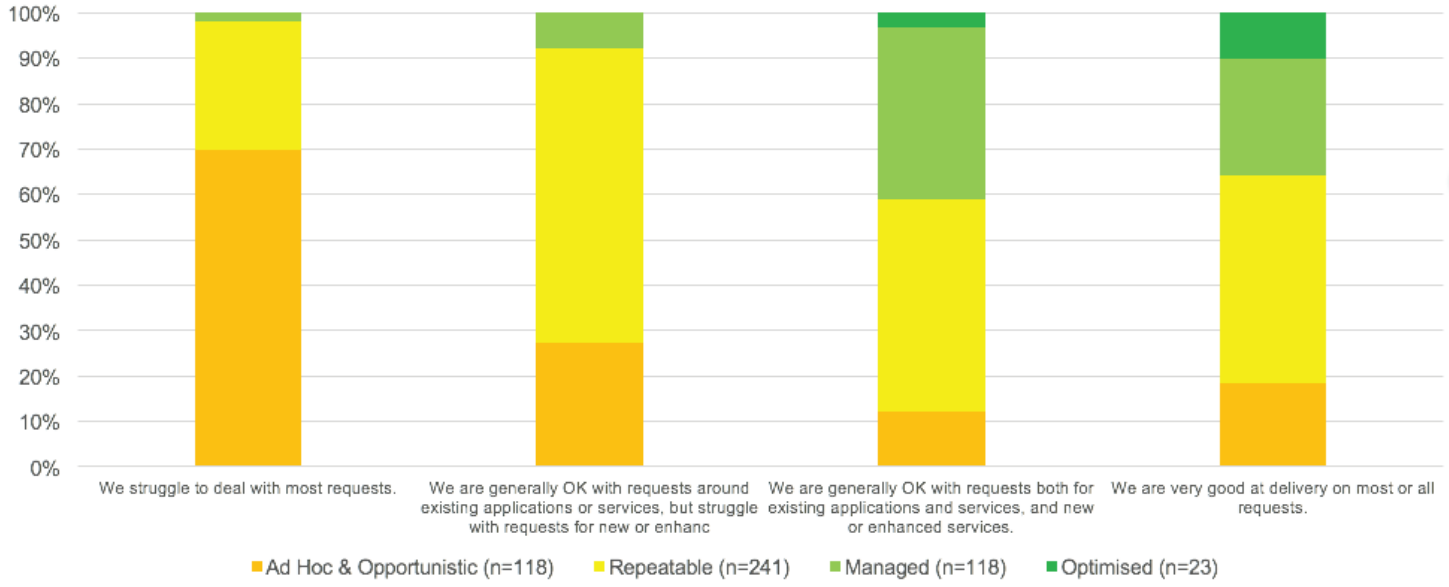


Figure 4 *Source: IDC, 2016*

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 or routine and repetitive activities can be automated to reduce pressure on limited or high cost human 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.