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?

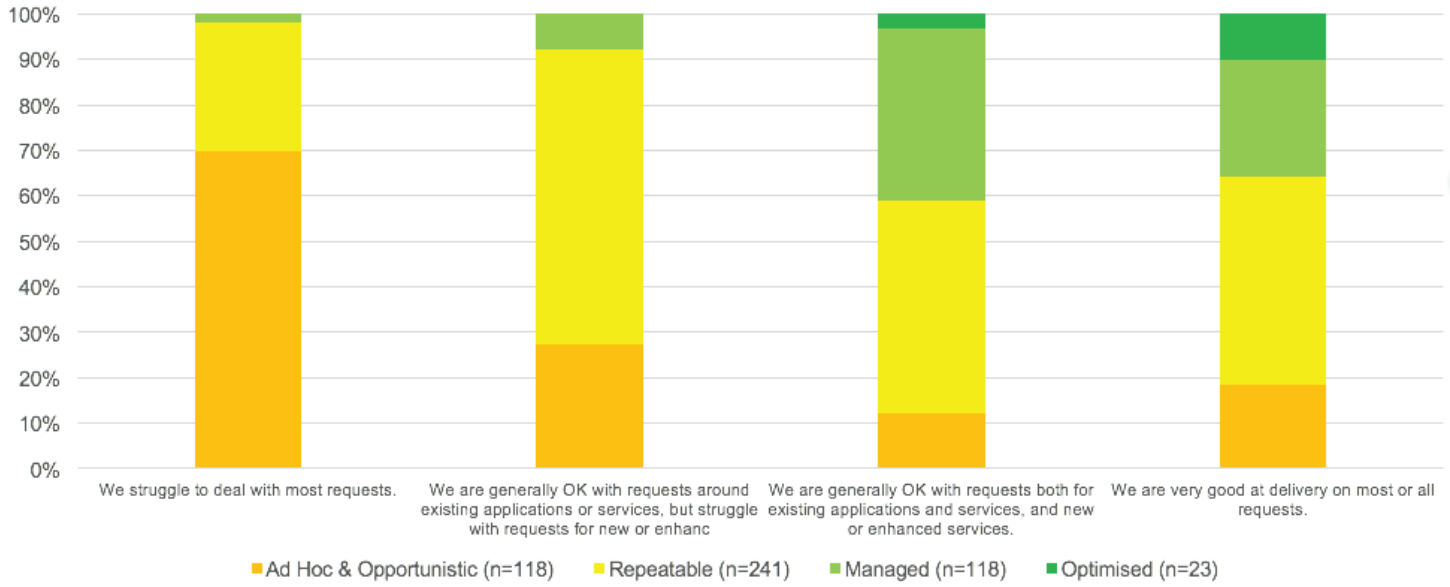

Figure 4 *Source: IDC, 2016*

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 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.**