www.pwc.com/me/cybersecurity

A false sense of security? Cybersecurity in the Middle East

Global State of Information Security® Survey

March 2016

pwc

Table of contents

Introduction

Cyber-crime is not a new phenomenon, but it's hitting the headlines as never before, with organisations across the world suffering high-profile and damaging breaches. Groups ranging from terrorists to activists have also made use of the internet, so the issue spreads far beyond economic crime. It's no surprise, then, that the World Economic Forum and Business Continuity Institute see cyber as a major business risk at the moment, or that cybersecurity has become a top priority, both for business leaders and for governments and law enforcement.

PwC has just conducted its latest Global State of Information Security® Survey covering 10,000 companies across 127 countries.

In this report we look at how the survey results from over 300 Middle East companies compare to those in the rest of the world.

Are the challenges here the same as those in other markets? And are companies in this region addressing them the same way?

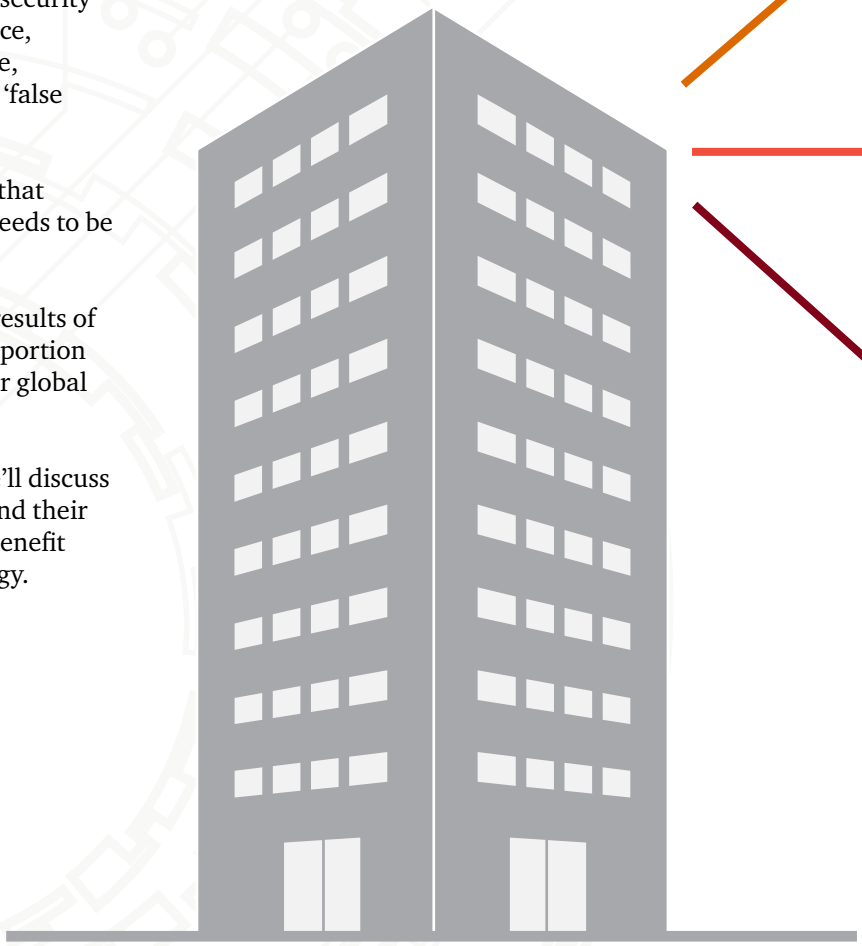
As we will see, Middle East companies do invest in security technology, and other things such as cyber insurance, however they are often not supported by the people, processes and governance required and so create a 'false sense of security'.

It's also clear from what these respondents told us that cyber's impact is broader than ever before, and it needs to be managed that way.

And as if the imperative to act wasn't enough, the results of the survey show that in the Middle East a large proportion of the companies also suffer bigger losses than their global counterparts.

As well as looking more in depth at the findings we'll discuss what companies here can do to make themselves and their assets safer, and ensure that they can continue to benefit fully from the positive potential of digital technology.

A broader approach to managing crime and cybersecurity:



It's not just a technology issue, **it's a business issue.** Digital is no longer the sole domain of IT and there are very real risks in allowing it to remain so: not just the risks of lost opportunity, but financial, commercial, and reputational risks too.

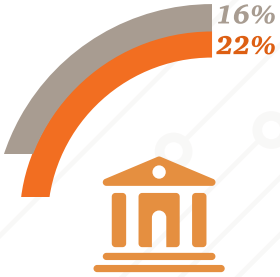
It's **a board-level issue.** Digital should report directly to the Board, and the Board should see it as central to their oversight responsibilities.

It's **an end-to-end issue**. From IT to physical security, from HR to IP, from Legal to Procurement: there is no aspect of modern organisations that is beyond its scope.

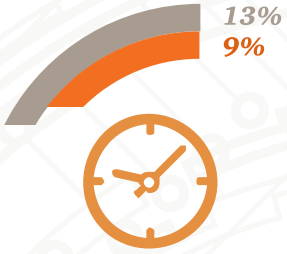
Cyber incidents

The impact of attacks:

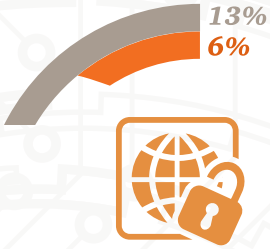
experienced losses of >500K USD



experienced brand/ reputational damage



experienced downtime of 3 days or more



experienced between 5,000 and 99,999 incidents last year

Middle East respondents Global respondents

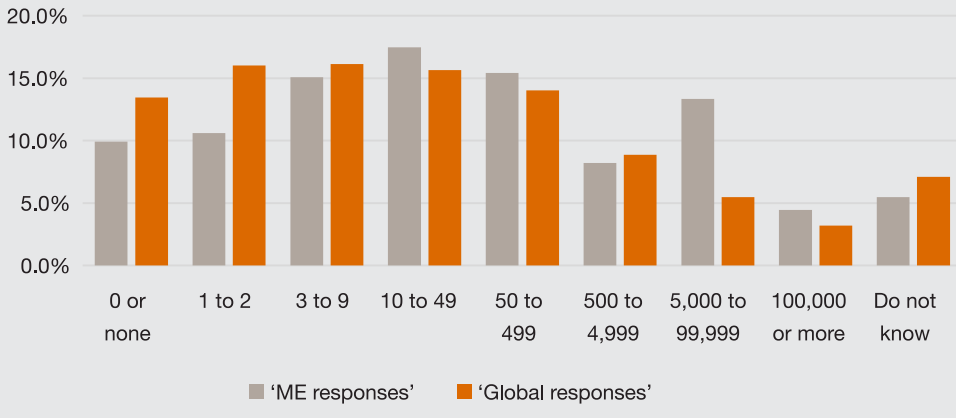
Middle East: More often, more severe

The headline finding is not good news. Companies in the Middle East suffered larger losses than other regions last year, as a result of cyber incidents: 56% lost more than $500,000 compared to 33% globally, and 13% lost at least three working days, compared to 9%.

Businesses in the Middle East are also more likely to have suffered an incident like this, compared to the rest of the world (85% of respondents compared to a global average of 79%). As the graph shows, the difference is particularly striking at the top end: 18% of respondents in the region experienced more than 5,000 attacks, which is higher than any other region, and compares to a global average of only 9%.

The attacks in question range from the actual theft of data, to co-ordinated spam emails or phishing attempts. One of the explanations for the high rate of such incidents in the Middle East may be the greater prevalence of malware in the region, and there are also more fax-based scams than is typical elsewhere, which can be hard for businesses to track centrally. Companies in general, as well as in the Middle East, often find it difficult to identify when an attack has taken place: many only discover it when third parties or clients report suspicious messages or requests for funds.

Number of incidents in the past 12 months



Why current cybersecurity measures fail

Such findings are a cause for concern, but all the more so because many companies in the region have invested significant sums in cybersecurity measures. And while they clearly lag their international peers in some respects, they do have many of the same measures in place. For example, 85% have established a globally recognised security framework, compared with 88% globally, and 24% have an information security strategy, compared with 25% globally. But that being the case, why are there still so many incidents in the region? The answer, in our view, relates to the three issues we've already discussed in relation to the global findings:

- **Technology isn't the answer on its own:** Middle Eastern companies can have a greater tendency to believe they can fix cyber issues by buying a technological 'fix'. But that needs to be supported by a parallel investment in awareness and training - less than 20% have a strong awareness programme, for example.
- **The board need to get involved** and there won't be real progress unless this happens. So even if 24% have security strategies, less than 15% of boards are behind them, and many of those strategies are too narrowly defined, relating only to IT and not to the wider impact of digital.
- **Cyber needs to be addressed on an end-to-end basis**. This is related to the previous point: a lot of firms in the region still see cyber as solely an audit or IT issue, but it needs to be integrated into the company's overall approach to security, which includes issues like HR, as well.

Cybersecurity

Technology: Necessary, but not sufficient on its own

Like other companies across the world, firms in the Middle East are investing significant sums in the technology of cybersecurity. However, the survey results suggest that, unlike elsewhere, companies in the region are relying too exclusively on technology alone to be the 'fix'.

Systems are clearly an important element of any cybersecurity programme, but they are not enough on their own.

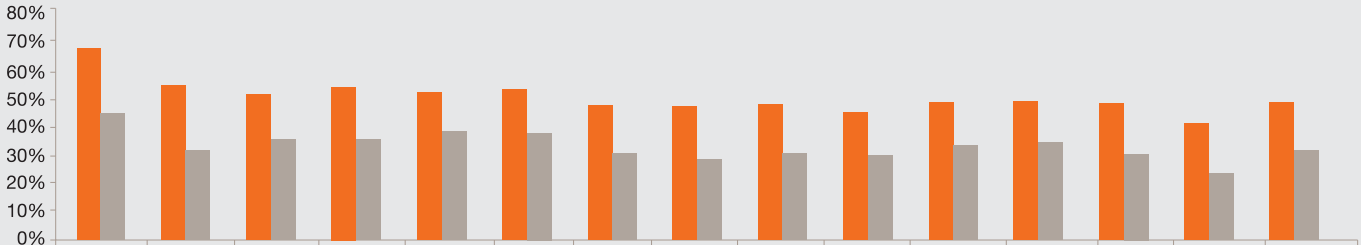
Like so many other business issues, cybersecurity is multi-dimensional. Technology is a key part of the mix, but only once the basics are in place around people, governance, and processes.

As shown, companies in the Middle East are in the top ten in the world in terms of their investment in cybersecurity technology, but in the bottom 50 for education and training in this area. This is where companies in the region could be focusing their efforts.

Technology needs to be used properly, with investment going into systems that fit the company's size, sector, and risk profile. These systems then need to be embedded into the way the business operates, rather than simply bolted on, and that includes education and awareness. Otherwise the risk is that senior management believe they are more fully protected than they actually are.

It's vital, for example, to change default passwords on any new equipment, and support the installation with the right staff training.

Which safeguards does your organisation currently have in place?



	Data privacy: Employ chief privacy officer (CPO) or similar executive in charge of privacy compliance	Data privacy: Require our employees to complete training on privacy policy and practices	Data privacy: Accurate inventory of where personal data for employees and customers are collected, transmitt.	People: Employ chief information security officer (CISO)in charge of the security program	People: conduct personnel background checks	Process: Employee security awareness training program	Process: Identity-manage-ment tolls	Process: security strategy for cloud computing	Process: security strategy for mobile devices (e.g.,smart-phones, tablet comput-ers, etc.)	Process: security strategy for Big Data	Process: classification of business value of data	Process: Threat-intelligence subscription services	Process: Active monitor-ing/ analysis of informa-tion security intelli-gence (e.g., vulne rability reports, log files)	Technology: Behavioral profiling and monitoring	Technology: Security-event Correlation tools
Global average response	67%	55%	51%	54%	52%	53%	48%	47%	48%	45%	48%	49%	48%	41%	48.%
ME average response	44%	32%	35%	35%	38%	37%	31%	28%	31%	30%	33%	34%	30%	23%	32%

People

There are a number of elements to consider here, and training is one of the most important. While human error is still a major cause of security incidents, only 37% of respondents in the region have a comprehensive security and training awareness programme (compared with 53% globally), and only 32% require employees to complete training on privacy policy and practices, compared with 55%. It's clear that more investment needs to be made in this area.

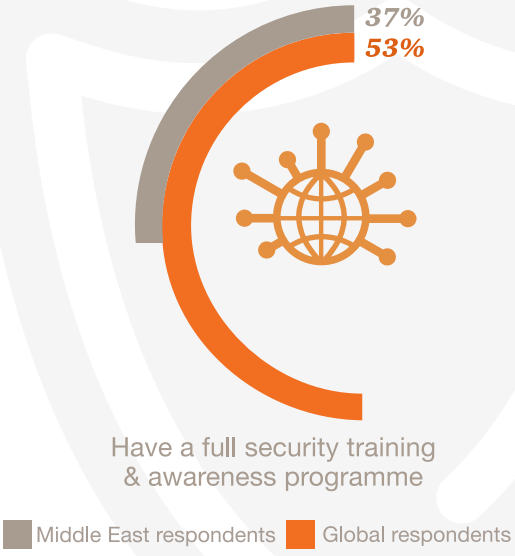
Recruitment is another issue: it can be a challenge to recruit top talent in the region, and digital is an area where the global demand exceeds supply.

Finally, a point linked to governance: cybersecurity needs to be managed at the right level, with the right level of seniority. Companies in the Middle East have a way to go here: only 35% of the survey respondents said they have a designated CISO or CSO responsible for security, compared with 51% globally, and those that do have such a role usually confine it to the IT department, and rarely give it the authority it needs. Only 11% are involved in reviewing roles and responsibilities (compared with 26%), and 14% are involved in communications or the identification of key risks (compared with 32%).

37%

of Middle East respondents have a comprehensive security and training awareness programme

The underpowered CISO or CSO in the ME



Governance

Good governance is partly about having the right people in the right roles, but it's even more important to have the right structure. This ensures leadership, accountability, and transparency. As we've discussed, 85% of respondents in the Middle East have adopted a recognised information security framework. The challenge, however, is that these frameworks are seen as 'just an IT issue', which means they are not aligned with the way the business actually works, and – crucially – do not support or reflect the company's commercial priorities. Cyber strategy needs to sit in the right place in the business, and be executed laterally, across all departments, rather than vertically, in IT alone. Only 38% of respondents in the region manage cybersecurity issues and communications through a cross-functional team, compared with 49% globally, and only 50% say their security spending is aligned with the business, compared with 67% globally.

Clearly cybersecurity is no longer just an IT issue, if it ever was. As recent events have proved, cyber incidents can damage every aspect of a business, from its physical and financial assets, to its brand and reputation. It's crucial, therefore, that cybersecurity is assessed, managed, and monitored like any other business risk. That means a governance structure that goes right up to Board level, as well as active oversight from the Board. While this is becoming the norm elsewhere in the world, it is not yet the case in most parts of the Middle East: only 56% of respondents in the region have an executive champion in this area, compared with a global average of 73%. Likewise only 25% of respondents' Boards are involved in cybersecurity strategy, and 25% in policy, compared to 45% and 41% globally.

There are a number of factors in play here, which reflect the distinctive business culture in the Middle East. For example, a very large proportion of the region's companies are privately or family owned with no external shareholders, which can mean that their Boards focus on profits, seeing controls of any kind as a drag on growth. The ownership structure also means there is often an intense concern about the firm's public standing.
The key point here is that cyber can threaten all of these things: it can cost serious money, impede the company's ability to expand and attract new customers, and damage both its assets and its reputation. The region needs a change in mind-set to reflect that very commercial reality, and all the more so, as the Middle East starts to face the challenge of falling oil revenues. Government spending will inevitably come under greater pressure, and some authorities in the region are looking at new ways to increase revenue, such as the introduction of VAT. In this new economic environment, cybersecurity measures will need to offer demonstrable value for money, and prove their efficacy more than has been the case in the past.

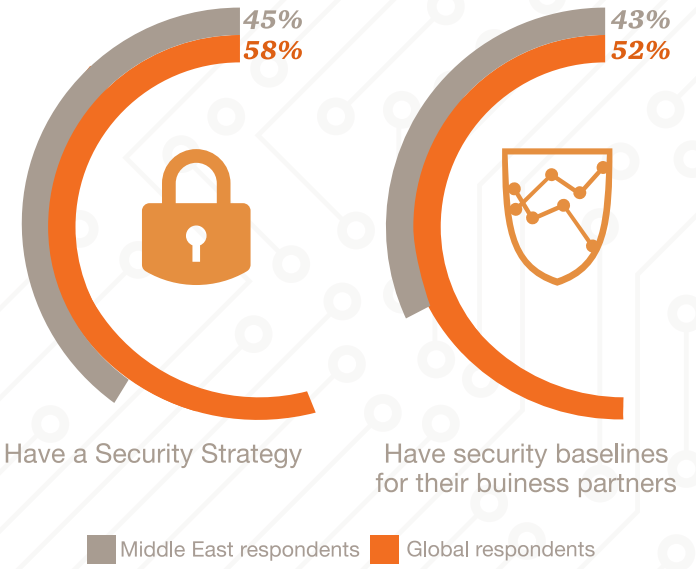
Another important factor for the future is the possibility of a more rigorous regulatory environment in markets like Qatar, Kuwait, the KSA, and the UAE, and authorities across the world are strengthening their regulatory frameworks, and intensifying the level of scrutiny. Companies could soon be required to appoint CISOs who report directly to the Board, for example, and establish recognised security frameworks. As we have seen, many Middle Eastern companies already have these things, but they are not operating at maximum effectiveness.
There are two key issues to consider in relation to the practical impact of any new regulation – the first is that regulatory authorities like the US and EU are likely to move faster, and demand more, than those in the region, and Middle Eastern companies with international operations will probably come within their scope (as the recent EU Court of Justice 'safe harbour' ruling proves). The second is whether any new regional regulation will be little more than box-ticking, or something more substantive.

Processes

The Global State of Information Security® Survey looked in detail at the various processes connected with cybersecurity. In almost all respects, the Middle East is falling behind the rest of the world. Areas of particular concern include identity management (31%, as against 58% globally), threat assessments (33% against 49%), vulnerability assessments (36% against 48%), security standards for external business partners (43% against 52%), and the active monitoring and analysis of cybersecurity information (30% against 48%). And while companies in the region are acutely aware of the threat posed by insiders, only 38% perform proper background checks on their personnel, against 51% globally.

This reinforces the point we made earlier: Middle Eastern firms need to think about, and manage, cybersecurity as a business issue, not just an IT issue. Identity management, for example, is not just a technological mechanism, it goes to the heart of business operations: companies need to know who they're dealing with, and that's more true now than ever before.

Identity management goes to the heart of business operations companies need to know who they're dealing with, and that's more true now than ever before.



Good processes help companies detect cyber incidents, and prevent them from happening, but they're also key to an effective response if an incident does occur. This is another area where cybersecurity in the region is often stuck in an IT silo. But this is a dangerous isolation. As we've learned from the high-profile breaches of the last few months, cyber-crime needs to be managed in the same way as any other threat to business continuity, and owned at Board level. This means detailed planning, scenario exercises, response management, and crisis preparedness, involving a wide range of functions such as Legal, HR, Forensics, Risk, and Communications. As we've discussed before, cyber is an end-to-end challenge and it needs an end-to-end response.

Companies in the Middle East - like those elsewhere - need not just the right technology, properly adapted to their business, but the right people, the right governance structures, and the right processes. Because without those things, they will be more vulnerable to future threats than they are probably yet aware.

Looking ahead: Fit for the future?

The pace of change in technology is quickening, and the world is becoming ever more connected. This is opening up new business opportunities, and new business risks. Companies in the Middle East are keen to exploit the potential of digital, but they don't as yet have a full or detailed understanding of the associated risks. As we discussed earlier, many buy new technology (both for security purposes, and in other areas of business) but don't then support it with the necessary training or skills. This means cyber in all its forms presents a greater threat to them than to their international peers.

Managing future threats

The Internet of Things

And all the more so because the world is converging. With fridges able to order milk from a supermarket, and smartwatches sending patients' health data to doctors, we're already living in a world where devices can communicate with each other without human interference.

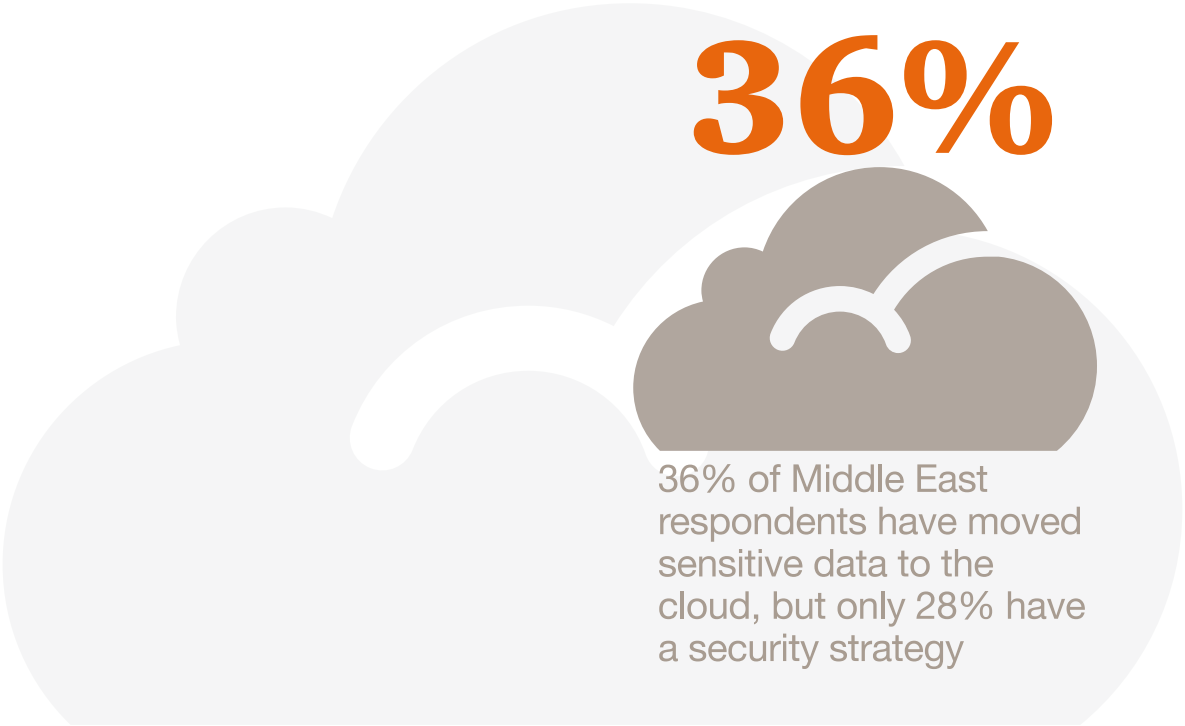
This is sometimes called 'the Internet of Things', and it offers vast opportunities, but equally significant risks in relation to complexity, uncertainty and trust, as companies in the Middle East have already discovered. Linking up smart meters in customers' homes, for example, poses significant risks to utility companies.

Similar issues can arise with loyalty cards (which have caused problems for airlines in the region), and even for apparently unsophisticated equipment like office coffee machines operated by third parties, where these are linked to the main IT infrastructure.

The cloud

The cloud presents similar challenges. More and more organisations across the world are moving applications, data or infrastructure onto the cloud, and as this gathers momentum it's likely that all companies will eventually use it in some way, as retaining some of these functions in-house will become less and less cost-effective. But doing so demands a high level of trust in the cloud itself. Those hosting such systems – be they governments or cloud providers - need to ensure they have the right protection and safeguards in place, and many will need to comply with US or EU legislation, given the global nature of their clients. Middle Eastern companies want to exploit cloud technology– and some already are – but they need to ensure their own internal security processes and systems are robust and resilient before they entrust important data to third parties. With this in mind, it's worrying that 36% of respondents in the region have already moved sensitive data to the cloud, but only 28% have a security strategy to cover it.

In our view, the number of challenges companies need to address is only going to increase as technology, business models, and global regulatory and legislative agendas evolve, and as demographic change has an impact on consumer behaviour. There will be increasing complexity, uncertainty, and scrutiny, and trust will become ever more important. Middle Eastern companies will be better placed to deal with these structural challenges. If they ensure cyber is addressed across the whole organisation, not just in IT; if the Board takes ownership of it; and if it's understood and managed on an end-to-end basis.



Critical assets

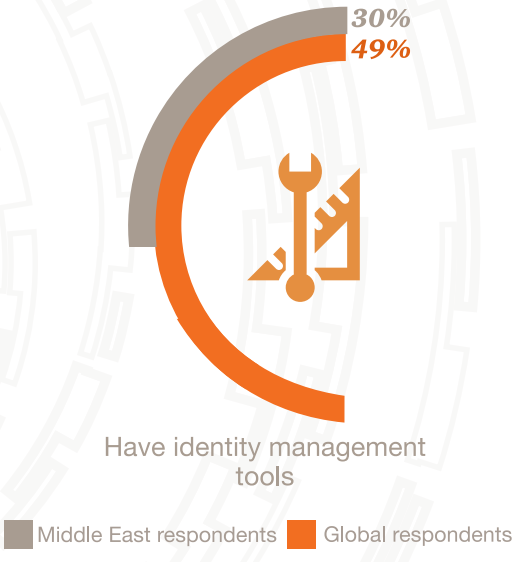
Companies can only move forward with confidence if they are clear what their critical assets are, and understand how these need to be protected. There's a growing use of 'cyber-insurance' in the Middle East region, with 47% already buying a policy like this. But there is a risk that this could be another example of a 'quick fix' which may actually create a false sense of security; such policies are only useful if they are covering the right things. Only 33% of respondents in the region have established what their 'crown jewels' are and this should be an urgent priority for the remaining 67%. There also needs to be an acknowledgement that which assets are 'critical' will evolve on an ongoing basis.

Identity management

The emerging digital era is driving an ecosystem of porous perimeters, where customers, suppliers, providers and regulators interact seemlessly with a business. Ensuring identities are correct and protected will be essential for security.

In the Middle East, identity management is recognised as important area of investment. Currently only 30% of Middle Eastern respondents had implemented identity management tools, compared to a global average of 49%, and nearly all Middle Eastern entities with identity management outsource this capability (compared to a global average of 21%). 27% of Middle Eastern respondents have prioritised identity management over the next 12 months (compared to 20% globally).

In an interconnected world, identity is not just about people. The "Internet of Things" phrase is already being replaced by the Internet of Everything, where devices like your watch, fridge or heart-rate monitor will automatically communicate with other devices autonomously and without human interaction. For organisations, this will drive efficiencies and new ways of doing business, driving logistics and procurement chains, monitoring of health, transport, utilities and finances. It will also open vulnerabilities around managing the identities of devices.



Trust

Trust has always been vital in business, and in an increasingly digital commercial environment, trust is more important than it's ever been; trust between companies and their business partners, and trust between consumers and the companies they buy from online. Brands that have been built for decades can now be destroyed overnight if people no longer think their personal data is secure.

Trust is particularly important in the Middle East, where so much business is based on personal networks, and commercial relationships that sometimes go back generations. But 34% of respondents in the region have little or no confidence in the security of their business partners' information security.

Companies in the Middle East are also noted for their concern to protect their privacy and keep their commercial activities confidential. This is hampering the effective sharing of information about actual and potential security threats, which means attacks can proliferate, and the impact be more severe.

Conclusion

Global organisations continue to grapple with the cybersecurity challenges emerging in our newly interconnected world. These challenges are only likely to increase, given ever greater connectivity, the convergence of technologies, more assertive regulatory and legislative agendas, and the emergence of a new generation of 'digital natives', who are more conversant with technology, and happier using it.

Nowhere will this be more important than in the Middle East, and the region faces its own particular challenges. Organisations here already face a disproportionate level of attacks, and suffer more consequences from them than companies elsewhere in the world. This has led to a sharp rise in spending in security technology, but without the necessary supporting investment in improving awareness, governance, and processes. At the same time, the Middle East is one of the world's most advanced regions when it comes to the speed of technology adoption, and as its youthful populations go online and technologies converge in the Internet of Things, there will be new risks – and even greater ones – than the region is already facing.

What organisations need to do differently

Organisations in the region will be more resilient in the face of these risks, and will better placed to exploit the potential of new digital technology if they approach cyber on the following basis:

- It's a business issue, not an IT issue, and needs to be managed as such
- It's a board-level issue, and those on the Board need to understand it, be trained on it, and actively oversee it
- It's an end-to-end issue that brings in functions like Legal, Communications, Crisis Management, HR, and Risk within the business, as well as partners and suppliers outside.

How we can help

We provide a comprehensive range of integrated cybersecurity services that help you assess, build and manage your cybersecurity capabilities, and respond to incidents and crises. Our services are designed to help you build confidence, understand your threats and vulnerabilities, and secure your environment. Our cybersecurity service delivery team includes incident response, legal, risk, technology and change management specialists.

Methodology
About the survey

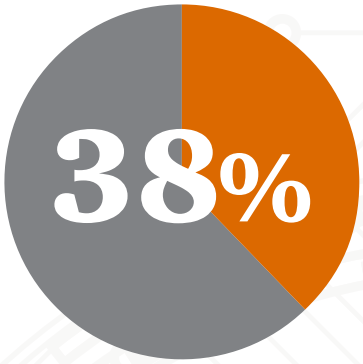
The Global State of Information Security® Survey 2016 is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from May 7, 2015 to June 12, 2015. Readers of CIO and CSO and clients of PwC from around the globe were invited via email to participate in the survey.

The results discussed in this regional report are based on responses of more than 300 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 20 countries including Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, United Arab Emirates, Algeria, Afganistan, Angola and Tunisia.

Appendix A: Responding to rising cyber-risks

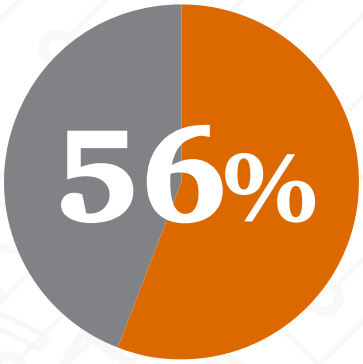
Insights from The Global State of Information Security® Survey 2016

Average number of security incidents



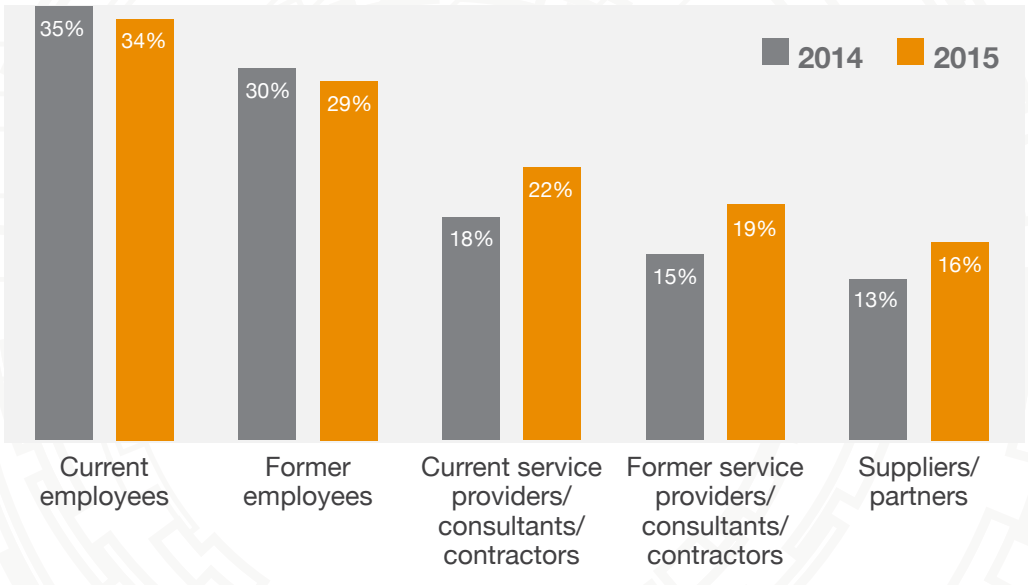
In 2015, **38%** more security incidents were detected than in 2014.

Impacts of security incidents



Theft of "hard" intellectual property increased **56%** in 2015.

Sources of security incidents



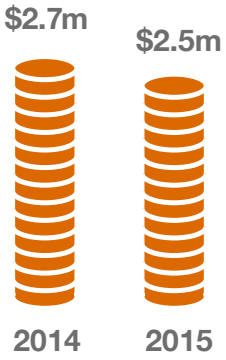
22%

While employees remain the most cited source of compromise, incidents attributed to business partners climbed **22%**.

Average information security budgets

Respondents boosted their information security budgets by 24% in 2015.

Average financial losses due to security incidents



-5%

Financial losses decreased 5% from 2014 to 2015.

Adoption of strategic security initiatives

Many organizations are incorporating strategic initiatives to improve security and reduce risks.

Contact details

PwC offers both strength in depth, and strength in breadth in the management of cybersecurity. We can help you develop an effective strategy, assess your IT needs, establish robust governance and processes, and implement an efficient action plan that involves stakeholders across the business.

Middle East

Mike Maddison
Partner, Middle East Cyber Services Leader &
Head of Risk Assurance Services
mike.maddison@ae.pwc.com

Wasseem Khokhar
Partner, Legal Services
waseem.khokhar@pwclegal.com

Nick Robinson
Partner, Middle East Forensics Leader
nick.robinson@ae.pwc.com

Taha Khedro
Partner, Advisory Technology
taha.khedro@ae.pwc.com

www.pwc.com/me/cybersecuirty

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

Creative Design Centre CDC1175 032016