INTEGRATED SOLUTIONS OFFER THE KEY TO SUCCESSFUL SECURITY

CIOs in the Middle East search for a tightly meshed security ecosystem to meet the changing demands of business today and defend against a growing variety of threats

Survey conducted by IDG Connect on behalf of RSA
The Middle East's IT leaders say they are not well prepared to deal with the onslaught of challenges to information security but see big business advantages in fixing that state of affairs.
INTRODUCTION

Cybersecurity is the threat that never goes away but organisations must strive to continually improve their awareness of the threatscape and bolster their defences against those challenges.

In order to get a picture of what is happening with cybersecurity in three countries in the Middle East, RSA commissioned IDG Connect to conduct a survey and report back on what it found in terms of perceived issues, attitudes, preparedness, investments and effective defences.

IDG Connect interviewed 100 senior IT decision makers in the Middle East region. Saudi Arabian business technology leaders made up the majority of the respondents (38%), followed by Qatar (33%) and United Arab Emirates (29%).

The majority of survey participants worked for organisations with 500-999 staff (62%) and 38% worked for large organisations with staffing levels of 1,000 to 4,999. Those polled were all senior decision makers, with information technologists making up 92% of respondents, and the remaining 8% in finance roles.

Three industries made up the bulk of respondents by vertical market: 28% of those surveyed are in retail, 26% in financial services and 20% in the energy and utilities market. A further 13% of respondents came from the telecommunications industry, 10% from healthcare and 3% from the public sector.

What did we find? In short that most organisations do not feel well prepared and that they struggle with a rapidly changing business and technology environment. A couple of issues stood out: a more integrated approach is seen as most likely to deliver effective defences and if organisations can get close to the ideal state of readiness they see major advantages to their businesses across the board.
A NEED FOR INTEGRATION

Today’s CIO operates a technology estate that is of a wider scale than at any other time in business technology history. CIOs and their teams must operate at multiple speeds to both innovate and protect. They support a mix of owned and operated platforms, outsourcing contracts, cloud services and, increasingly, a number of point-solutions chosen and procured by line-of-business managers outside of the IT department. In the last five years the single-vendor deal providing a full range of products and services has all but disappeared as CIOs have sought new ways to enable the organisation to achieve its goals. As a result, a diverse culture of technologies, needs and suppliers exists within organisations. But this diversity and complexity has opened up gaps in information security.

Just as the number of applications to operate the business and serve customers has grown, so too has the number of products organisations use to secure and protect their intellectual property, customer data and operations. Our study demonstrates that just as CIOs are seeking cloud management platforms to integrate the various services they use, so too are they seeking an integrated security platform from which to moderate threats and secure their businesses.

Almost nine in 10, 88%, of respondents are using multiple systems to detect and manage security breaches, with threat analysis and a firewall being the most commonly used services, covering over half of the audience (55% and 51% respectively). Just under half reported that threat management, anti-spam and identity management tools were the next most prevalent platforms in their organisations.

We found that not only is threat analysis commonly used but 22% of those taking part believe it delivers the greatest impact to their organisations, followed by identity management by 15%.

When asked what approach has the greatest positive impact on the security of their organisations, respondents demonstrated their desire for an integrated platform that supports a wide variety of security tools. But today no single security system achieved more than a quarter of responses and instead respondents highlighted a broad sweep of tools they felt would have the greatest impact. After threat analysis and identity management, threat remediation was identified by 10% of those taking part, while anti-spam and threat risk tools were both identified by 8% of the survey group. Threat management, firewalls, end-user compliance processes and anti-virus tools were all cited by 7% with encryption and access control completing the analysis with four and three percent respectively.

This chart clearly shows that the CIO community in the Middle East is looking at their broad security threat landscape and do not believe that there is a ‘silver bullet’ point solution.
We've said already that security challenges come from all around so we asked a follow-up question about how security tools worked with other security tools - and the answers were illuminating. Only threat analysis systems scored remotely highly here with 38% but the next highest score was just 27% and that was for end-user compliance training and processes. This begs the question: if organisations don't feel that their current security tools knit well together, how can they possibly feel confident in their ability to withstand threats?

This finding might well suggest the way that security systems have been accreted in piecemeal fashion over the years from various vendors, many of which have been later acquired but not necessarily integrated with the parent company's other security assets. Different code bases, user interfaces and so on can make creating a unified set of security defences a major challenge for vendors as well as IT buyers.

CONNECTING THE DOTS

The survey showed that CIOs in the Middle East are witnessing a high number of cybersecurity threats. Almost all (97%) see three or more threats and all possible answers polled at 65% or higher. Nearly four in five of those responding said denial-of-service attacks were a high security priority and 77% nominated controlling internal risks. Clearly in a post-Edward Snowden age there is increased recognition of the threat of "the enemy within" – trusted employees or contractors who have privileged access to systems. But what is notable here is that threats are across the board, with identity theft, spam, spear phishing and virus threats all cited by a significant majority.

"Cybersecurity is an expanding bubble and in that bubble the ways you can be attacked are increasing," says IDG Connect principal analyst Bob Johnson of the results.

The geographic breakdown here is interesting with 80% in Qatar seeing spam as the most prevalent security priority. There's another standout figure when we come to a vertical industry breakdown: the energy sector is clearly plagued by spammers as 90% listed this as an issue. These numbers once again point to the importance of a unified approach where integration between defences and a central policy represents best practice.
GAINING VISIBILITY

Given the complex and fragmentary nature of modern information security, visibility plays a huge role in the lives of CIOs and CISOs so we asked our audience how far they felt they could see into their networks and systems today to detect intrusions but also to avoid alarms caused by false positives.

Tools for detecting network outages were the number-one answer, cited by 54% of respondents, followed by those for checking service levels and ensuring operational compliance (50% each) and then critical access, malicious site access, non-compliance and application outages.

But then when we asked a supplementary, forward-looking question about where more visibility is needed we gained another perspective. One area that clearly needs redress is outside probes, which both scored the lowest for providing visibility today (34%) and easily the highest when it came to most need for increased visibility (39%).

Over 90% of the organisations taking part have at least three security tools to give them greater visibility of the threat landscape they face and a view of the false alarms and general intrusion detection. All answers achieved significant response levels at 34% or higher.

When viewed by nation, there were some notable splits. Respondents in Saudi Arabia saw tools indicating non-compliance as providing most visibility but in Qatar detecting outages and operational compliance ranked equal highest.

Breaking the results down by vertical markets, the retail sector, which includes online-only retailers, saw network and application outages and service level performance as the lenses they used most for security visibility. In financial services, which includes professional services like accounting, network outages was seen as the most successful security visibility approach, along with service level performance and critical access. In the oil, gas and utilities sector operational compliance and malicious site access provided most effective views.
IDENTIFYING THREATS

In order to zero in on one of the big challenges of our time, identity and access management, we asked what factors were causing the headaches in this area. And clearly there are headaches, with 90% saying they experience issues in four or more areas and with a long list of other responses also receiving significant recognition.

But here, one modern area stood out from the pack: the seemingly inexorable rise of mobility and bring-your-own-device policies (cited by 50%), followed by recovery tactics and access to resources. Clearly, allowing users to select their own tools and work from multiple locations allows for great liberties and user satisfaction, as seen by many other surveys in the past. But this freedom of choice is also setting hurdles for IT and infosec bosses to leap, not least of which is getting policies and systems on who gains access to networks and systems right.

When we asked as a supplementary question which issue was paramount, mobile/BYOD was joined at the top of the list by false alarms, caused by systems wrongfully restricting access by detecting suspicious behaviour. This issue is by no means new and shows no signs of going away, judging by our research. The result of these alarms is time-consuming resets for already hard-pressed IT staff.

Most other answers were closely ranked and spanned everything from soft skills (user education, resources, tactics for recovery and dealing with complexity and with false alarms) to technical issues (inadequate log data and monitoring and reporting).

TOUGHEST CHALLENGES

Having gone narrowly in on identity and access management we broadened our view by asking about challenges to detecting and remediating threats. Once again there was evidence of an array of issues with 90% saying they had three or more challenges and all possible responses returning significant numbers.

Once again, mobile/BYOD was named as the most commonly cited challenge (72%) with cloud computing (69%) the second most quoted challenge, perhaps indicating that having applications and services located remotely poses a relatively new challenge for those IT shops accustomed to fixing matters in the comfort of their own datacentres.

The situation was reversed when we asked the audience to name their biggest single challenge, with cloud moving well ahead (see chart below). This is an interesting development. Mobile/BYOD and cloud computing are clearly powerful forces and often hailed as being at the centre of a new, more dynamic IT. But our survey suggests that tighter governance might be required to bridge the gaps they potentially open up.

Partners, users and service providers were also named but one interesting answer was Big Data. As more companies put huge data sets in the cloud or query them in new ways there is clearly recognition of scope for security challenges. Losing such assets and revealing sensitive data and key performance indicators could be a live threat as more companies invest in the analytics tools to probe vast troves of new and old information.

IDENTIFYING THREATS

Most important challenges to identity and access management

<table>
<thead>
<tr>
<th>Mobile devices/BYOD</th>
<th>False alarms</th>
<th>Staff skills</th>
<th>Recovery tactics</th>
<th>Access to resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>11%</td>
<td>11%</td>
<td>9%</td>
<td>7%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Threat detection and remediation

- Major challenges
- Most important challenge

<table>
<thead>
<tr>
<th>Mobile devices/BYOD</th>
<th>72%</th>
<th>19%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providers</td>
<td>45%</td>
<td>13%</td>
</tr>
<tr>
<td>Partners</td>
<td>50%</td>
<td>11%</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>69%</td>
<td>33%</td>
</tr>
<tr>
<td>Big data</td>
<td>52%</td>
<td>14%</td>
</tr>
<tr>
<td>Internal users</td>
<td>57%</td>
<td>10%</td>
</tr>
</tbody>
</table>
EFFECTIVE APPROACHES

As IT leaders seek roadmaps to plot their investment strategies for cybersecurity, they report high expectations for strategies which will help guide those capital expenditure options.

The good news is that almost the entire survey sample (99%) said they expect three or more approaches to deliver positive impacts over the next two years and all possible answers received significant responses.

And there is one outstanding answer here with integration of security systems indicated as delivering a positive impact for 59% of the survey sample, just below hardening the desktop administrator environment, which 60% of the respondents said would deliver a positive outcome.

Other areas of strategy that the survey respondents forecasted would deliver better cybersecurity were increasing Active Directory security (54%), new monitoring methods (52%), enforcing policies (48%) as well as predictive analytics (47%) and end-to-end solutions (47%).

But when we drilled down and asked what would be the most effective single approach the numbers changed and integrating security systems was deemed the number-one answer by far with 22% of those polled. This underlines our major leitmotif of this research: in security, integration of tools and approach is key.

Breaking down the numbers by regions and company size reveals disparate approaches. Well over half of those polled in the UAE (58%) thought securing Active Directory would result in a positive impact. And 61% of their peers in Saudi Arabia expected new monitoring methods to be beneficial. New monitoring methods was also seen as incurring a positive impact for business technology leaders in the financial services vertical market, according to 64% of respondents. But when analysed by organisational size, large businesses with 1,000 to 4,999 see enforcing policies as effective (63%).
Our response base acknowledged a wide variety of security gaps in their organisations in the Middle East. The survey found that 98% have at least three major security gaps in their enterprises. These gaps fall into three categories: ability to adapt to changing business needs (52%), no “single pane of glass” view of the security of the organisation (52%) and an inability to prioritise cybersecurity investments (50%).

These gaps differ by geography. In the UAE, a “single pane” view of their security landscape and partner co-operation were each noted gaps for 65% of those taking part. In Qatar, tools and expertise were said to be notable omissions for 57% of those involved. When assessed by vertical, the absence of that single pane view is a gap for 73% of retailers. And 71% of those in financial services believe insufficient investment is an issue. For their peers in the oil, gas and utilities sectors insufficient investment is also a noted problem (52%).

When we asked a subsidiary question as to what is the top priority to address, ability to adapt to changing needs was by far the biggest response with 19% and the rest of the responses were bunched together. This is emblematic of what’s going on today: organisations need to deal with a world that is not programmatic, predictable and planned, but one where change is ongoing and where fluctuations in macro economies, industries and geopolitics can have very real effects on their ability to perform and to stay secure.

One more note that backs up our previous page discussion. Vendor cooperation is critical to success so suppliers need to build bridges with their customers and act more as a trusted counsel and true partner.
So what did we learn about the investment plans of the survey respondents? It is unsurprising given the increasing threat landscape that these organisations face that cybersecurity investment budgets are increasing, with 80% of those taking part in the survey saying they expected their spend to rise. This backs up the thought that there might be only three certainties: death, taxes, and security spending...

Increased investment in threat management – that is, focusing on current events – is being planned by 81% of those taking part in the survey but risk management (concerning future challenges) and threat analysis (concerning past events) are also expected to increase (71% and 52% respectively) for a majority of respondents.

However, when we examined areas where security spending will be decreased there was an interesting discovery. Over a quarter of respondents (27%) will reduce spend on threat analysis, compared to just 15% on risk management and 12% on threat management. This demonstrates possibly that respondents are focused on analysing current, and anticipating future events, and spending less time, money and energy on trying to learn from past events.

The picture is played out when the survey figures are looked at in a more granular way. In the UAE over one third (35%) of respondents plan to decrease investments in threat analysis and the same story is told in Qatar with 34% also decreasing threat analysis investment. In financial services, just 39% plan to increase threat analysis investment.

Investment priorities will therefore change with threat management and risk management both expected to see investment increases but there are some interesting differences.

Given its importance to the economies in the Middle East, it is perhaps not surprising to learn that the oil, gas and utility sector expects an overall 16% total increase in cybersecurity investment over the next two years.

Respondents rate their cybersecurity preparedness at 54 on a scale of one to 100 but see adequate preparedness significantly higher at 65. Clearly our audience feels it is coming up short when it comes to having sufficient defences for dealing with today’s and tomorrow’s threats.

But our research also reveals a fascinating conundrum. Respondents say that if they reached a state where they were fully prepared across cybersecurity systems, policies and analytics they could expect to see big business benefits. These include highly significant employee productivity benefits that would equate to adding about 10 hours to the average productive working week. Very consistently similar increases would apply to customer satisfaction, system uptime, readiness for new business opportunities, speed at which they can innovate, process efficiency and effectiveness of communications.

This, as we have argued, is a conundrum but maybe also a sign of immaturity: the audience sees the advantages of being fully prepared but don’t feel they are there yet. Still, the high expectations of what full preparedness can deliver is a positive sign that security readiness can have a genuine effect on other aspects of the business.

We might compare this with the effects of the Sarbanes-Oxley Act and other governance mandates. Many organisations “cleaned up their houses” for compliance purposes but subsequently discovered that the requirements to carefully audit and measure business and IT activities gave them benefits in terms of visibility and process improvements.
This study demonstrates the complex nature of modern business and therefore the complexity of the role of a CIO and IT team. Today’s CIO has to deliver a stable operation that complies with regulations, is secure and yet also agile, using the latest technologies and methods. But the rate of change and diversity of the landscape that businesses and CIOs operate within creates security gaps.

The danger of these gaps is clearly demonstrated in this study. Almost everybody we asked admitted their organisation had multiple security gaps and they take many approaches and adopt many tools to give the CIO some semblance of an interconnected view of their security posture. Yet it’s abundantly clear from the study that those taking part do not feel these tools are collectively able to protect them adequately today, despite their seeing many advantages in being ideally prepared.

The surveyed community is tasked with meeting constantly changing business needs and at the other end of the spectrum an increasing array of security threats is challenging their teams. Technology changes such as the increasing use and demand for cloud technologies and mobility are further extending the security gaps that they fear will hurt them.

What this study highlights is that the leaders understand the complexity of the situation but see a need for a more integrated approach. Only by a having a thoroughly integrated portfolio of security tools and processes can they create a platform for greater visibility and a greater strategic ability to secure and advance the business.

CONCLUSION

Connect tools and approaches to gain a superior security posture

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 44 million business decision makers’ details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.