IDC Middle East, Africa, and Turkey, Al Thuraya Tower 1, Level 15, Dubai Media City, P.O. Box 500615, Dubai, United Arab Emirates (UAE).
Tel: +971 4 391 2741 Fax: +971 4 391 1922

WHITE PAPER

Impact of Cybersecurity Attacks and New-Age Security Strategies

Sponsored by: MEEZA

Megha Kumar
March 2014

IDC OPINION

Targeted cyberattacks in the Gulf Cooperation Council (GCC) countries, including Qatar, have increased in frequency and complexity over the past two years. The recent spate of attacks on energy and media organizations emphasizes the fact that these intrusions now have broader political and economic agendas.

Organizations in Qatar are beginning to acknowledge that cyberattacks have more severe consequences than just downtime. Companies can face financial loss and experience loss of customer or corporate data and loss of reputation; further, they can also be held liable for loss of data or services by business partners and customers. The need for robust security solutions is now more critical than ever.

These attacks have caused businesses to acknowledge the need for better information security strategies and solutions to help mitigate these incidents. Consequently, companies are looking into security and vulnerability solutions, including vulnerability assessments, security event and incident management, and digital forensic solutions. In addition, they have increased network monitoring; currently, they manage this task in house due to the limited availability of Security Operations Center (SOC) providers in these countries.

Organizations in most vertical markets are susceptible to cybercrime, and companies need to leverage threat intelligence to improve security and use SOCs to protect themselves better.

IN THIS WHITE PAPER

This IDC White Paper explores the evolving threat landscape, the challenges organizations face, and the need to leverage threat intelligence from SOCs to establish metric-based information security strategies. Additionally, it describes how MEEZA's SOC services are designed to alleviate some of the challenges organizations in this region encounter when establishing a robust security infrastructure.

Methodology

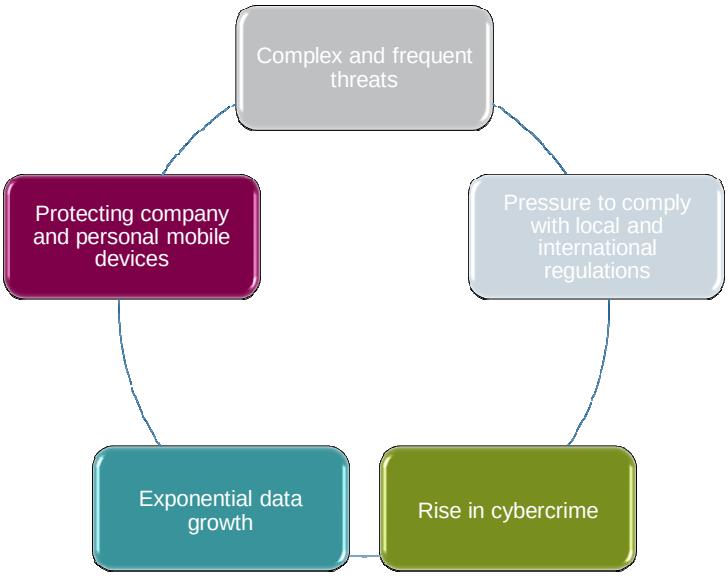
This IDC White Paper presents the results of a special IDC study commissioned by MEEZA. In preparation for this White Paper, IDC utilized its continuous research on information security practices in the region. IDC conducted a few in-depth analyst-driven interviews across the region with customers and information security vendors. On the vendor side, IDC interviewed major security solution providers. The customers were a mix of large banks, aviation companies, and oil and gas organizations. The objective of these interviews was to understand the drivers behind growing customer interest in security and to gain insight into the solutions they are adopting.

SITUATION OVERVIEW

Over the past decade, the threat landscape in Qatar has evolved dramatically with the growing frequency and increasingly sophisticated nature of cyberattacks. In addition, companies in Qatar have to work with the complications of securing new applications, mobile devices, and confidential corporate data while complying with the regulations of local and international authorities.

FIGURE 1

The Evolving Threat Landscape



Source: IDC

Information security has grown in importance for CIOs and IT decision makers in Qatar. Companies are beginning to acknowledge that, if they want to remain competitive and sustain uptime, they need to ensure the protection of their internal and external assets. Qatar has been one of the most proactive countries in the GCC in terms of corporate security, implementing security directives from the Supreme Council of Information and Communication Technology (ictQATAR) and the establishment of the Qatar Computer Emergency Response Team (Q-CERT).

However, despite all these factors driving information security adoption in Qatar, investment in IT security solutions tends to lag, as organizations face numerous challenges in establishing a secure environment.

In a recent study conducted by IDC, nearly 200 organizations across the GCC (including Qatar) were asked about the obstacles for IT decision makers in establishing secure IT infrastructure.

FIGURE 2

Top 10 Challenges for Information Security in the GCC, 2012

Source: IDC, 2012

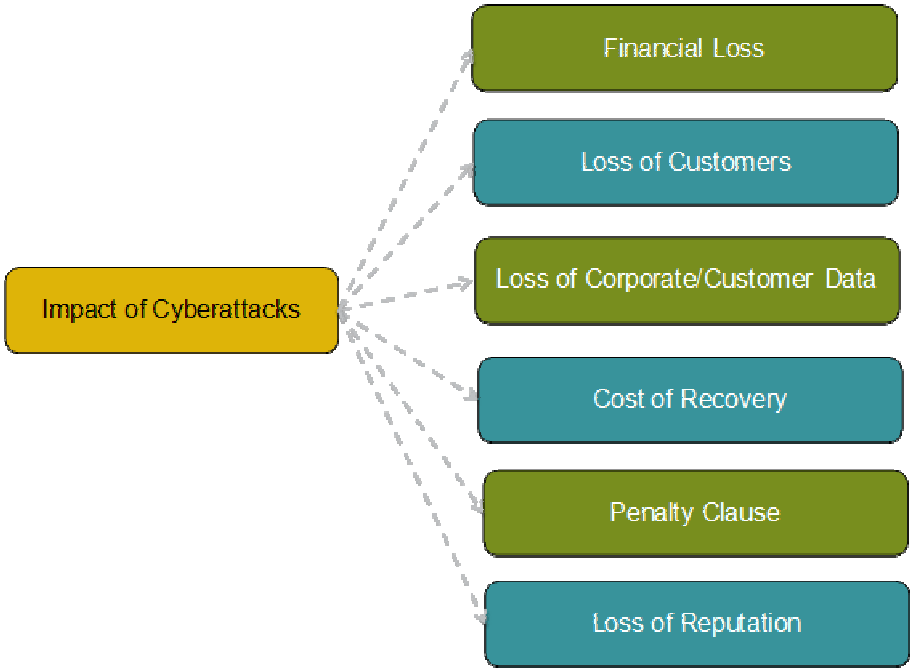
The results clearly highlight a lack of employee adherence to policies as a major deterrent to the establishment of a secure environment. Several companies in the region do not even have adequate security strategies in place; in addition, IT decision makers lack financial support from the business side of the organization and are forced to do more with shrinking budgets. These challenges lead to a very reactive attitude to security and vulnerable IT environments.

> *"While protecting the organization from external and internal threats is critical, some organizations in Qatar tend to ignore internal security and do not enforce proper security policies. Internal vulnerabilities should be a major concern, as these are the access points that lead to security incidents." – CIO, transportation vertical, Qatar*

While Qatar is, without doubt, home to a number of progressive and proactive organizations, other companies in the country tend to ignore the effectiveness of having a security strategy in place and do not understand the repercussions of a lack of security during a cyberattack. Most companies do not realize that these attacks cause far more damage than just shutting down services and compromising the effectiveness of security investments.

FIGURE 3

The Impact of a Cyberattack on an Organization



Source: IDC

Rise in Cybercrime

Cyberattacks have long since evolved from simple denial-of-service attacks to Advanced Persistent Threats (APTs). These threats are usually targeted, well timed, and aimed at impacting an organization or country on financial and political levels.

In 2012, Qatar became one of the first countries in the Middle East region to be subjected to cyberwarfare, with targeted attacks geared toward impeding the nation's energy and media sectors, creating economic and political repercussions. APTs of this nature are expected only to increase in frequency, and they attempt to cause the maximum damage possible.

Governments will also need to play a critical role when it comes to cybercrime, since they are among the main targets of APTs and are the main entities securing countries' telecommunications networks.

Organizations, including ictQATAR, have taken steps to secure the country and the business network by setting up cybersecurity research centers, establishing committees to investigate cybersecurity issues in key industries (e.g., energy) and running conferences and campaigns to educate users on the need for secure organizations and best practices.

Now more than ever, CIOs need to evaluate the cost of being compromised by a lack of a secure environment or proactive security strategy. Susceptibility to risk will

provide justification for increased security budgets, leading to the establishment of proactive metric-based security strategies.

> *"Given the recent attacks in the country, the attitude among executives in Qatar has changed; they now realize the need for security and internal training." – CIO, finance vertical, Qatar*

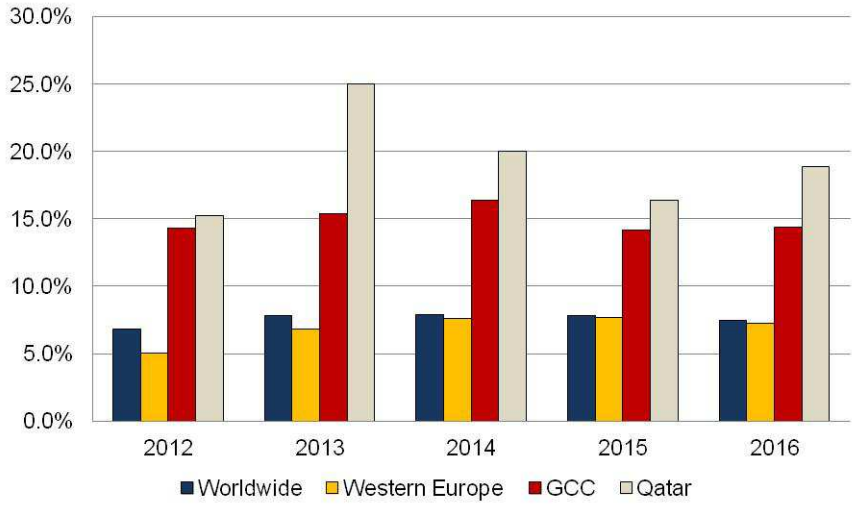
Implication of Cybercrime on Security Software Spending in Qatar

While it is accepted that cybersecurity threats will grow at an exponential rate in frequency and sophistication around the globe, the level of security spending in the GCC remains far more conservative than in mature economies. For example, in Western Europe, many companies have already undertaken high levels of spending on security software and will now seek to optimize their investments while working to achieve higher efficiency levels and ensure business availability.

Qatari organizations will invest significantly in security software solutions over the next three or four years, at a faster rate than the rest of the GCC. Although the motivation for this spending has arisen from the recent attacks on energy and media organizations in the country, Qatari organizations realize the need to ensure data security and privacy while investing in solutions to mitigate APTs better. Organizations in the country are beginning to acknowledge that the liability of not being well protected is not limited to downtime; it can have the additional repercussions of customer loss, failure to meet service-level agreements (SLAs), financial losses, and, most of all, loss of reputation and trust. An overall upward trend in security software spending is expected in the GCC in general and Qatar in particular.

FIGURE 4

Year-on-Year Growth of Security Software, 2012–2016



Source: IDC 2013

ESSENTIAL GUIDANCE

Creating a Metrics-Based Information Security Strategy While Containing Costs

A proper information security strategy will help an organization to remain proactive in managing threats and, most importantly, in ensuring business continuity. Information security strategies need to be planned, executed, and reviewed periodically.

An effective information strategy must address three major questions:

- How do we measure the value of IT security to the business?
- What is the risk portfolio of our business?
- How can IT security help in achieving business objectives?
- How do we manage the security and privacy of sensitive data when it resides outside of the corporate environment?

FIGURE 5

The Three Technology Pillars for Information Security Planning

Source: IDC

By answering these questions, organizations will not only establish an information security strategy, but they will also create a risk profile. Risk has become the single biggest driver for IT security planning, and, now more than ever, companies need to have more in-depth visibility into, and intelligence of, their IT infrastructures so as to ensure they can anticipate advanced threats and contain them accordingly.

Threat intelligence will become critical, and, by deploying the right tools and solutions, IT departments will be able to gather the necessary metrics to identify and understand:

- The security level of a network
- The number of open endpoints
- Out-of-date patches
- The impact of an incident
- The level of compliance with regulations
- Application vulnerabilities

The documentation of these findings will provide the justification needed to improve information security policies and help establish proper strategic and financial support from executive management, an issue that has been highlighted as a major challenge for IT decision makers in Qatar. These metrics form the cornerstone of an informed and proactive information security strategy.

> *"We perform quarterly reviews of our IT security policies and carry out both internal and external audits of our security environments on an annual basis." – IT director, finance vertical, Qatar*

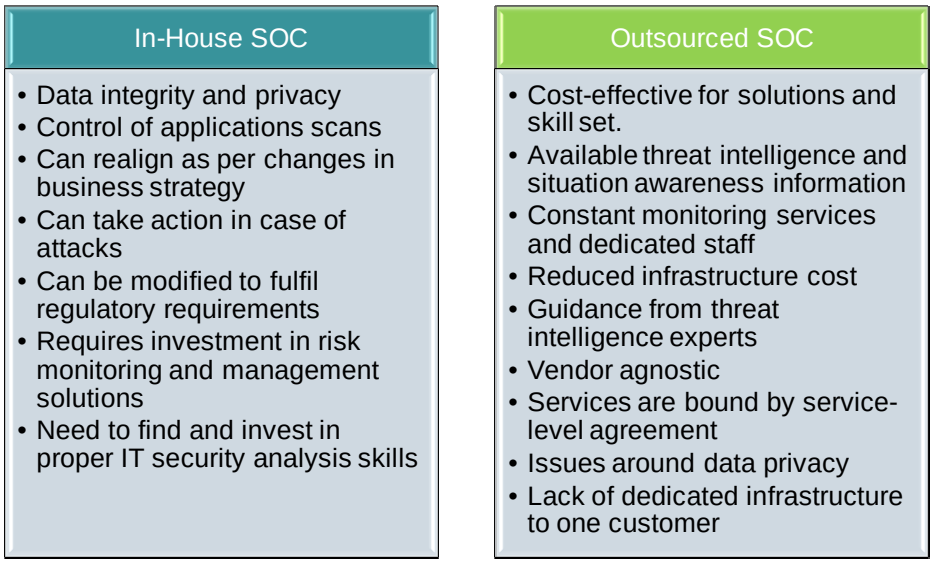
This need for threat intelligence leads to the expansion of the technology pillar shown in Figure 5, above, as companies will need to adopt solutions that enable them to be more proactive in mitigating threats, including vulnerability assessment solutions, security incident/event management tools, and establishing an SOC.

Security Operation Centers

SOCs are usually teams dedicated to addressing information security concerns and monitoring an organization's networks for vulnerabilities and attacks. SOCs can be established internally or the work can be outsourced to a vendor or an IT services provider with an established SOC.

FIGURE 6

In-House SOC Versus Outsourced SOC



Source: IDC

Cost is one of the most critical factors for an SOC. While regulatory considerations, the threat landscape, and the need for new technology solutions have all increased, budgets have not. Organizations are under cost constraints and need to evaluate the feasibility of keeping certain activities in house versus outsourcing them to a service provider. The same is true for SOCs; companies need to decide if they want them in house or use the services of an outside provider.

Large organizations in the region, especially those in the telecommunications and banking verticals, have been investing in their own SOCs. However, several companies IDC interviewed (apart from telecommunications providers) stated that network monitoring and conducting vulnerability assessments are two functions they are willing to outsource to a service provider. Currently, the GCC (including Qatar) has a limited number of regional-level SOC providers available, forcing these organizations to carry out these functions themselves. The use of SOC services would make the monitoring of internal and nationwide networks easier to manage and more cost effective, enabling resources to be dedicated to other major IT-related activities.

Given the low availability of skilled IT workers, companies should consider using the services of an SOC provider to monitor their network's health and raise awareness of any threats among business stakeholders. It should be kept in mind that, if a targeted attack occurs, most solutions help organizations mitigate the impact or prevent an impact to a certain extent.

MEEZA Solutions

MEEZA, a Qatar Foundation joint venture, is a provider of managed IT services in the Middle East and spans several vertical markets, including finance, government, telecommunications, energy, healthcare, education, and manufacturing, with an end-to-end solution delivery approach. MEEZA is becoming a recognized Systems Integrator and continues to establish itself with Smart City expertise.

MEEZA has Tier III-certified datacenters located in Qatar; these are known as M-VAULT 1, M-VAULT 2, and M-VAULT 3. M-VAULT 1 was launched in 2008, followed by M-VAULT 3 in 2012. M-VAULT 2 was launched in Q1 2014.

MEEZA's value proposition is its provision of the first commercial SOC services to the Qatari market. Through its SOC, MEEZA will be able to offer insight into the vulnerabilities and strengths of its clients' networks. The SOC will cover four major services:

- **Threat Intelligence:** This service will analyze networks and gauge the advanced threats prevalent within the GCC, warning clients on how vulnerable their networks are to these APTs.
- **Advanced Security Monitoring:** This service performs a correlation exercise on the customer's network at intervals, looking for instances during which the network security can be compromised.
- **Log Management:** This service will allow customers to keep a log of all activities on their networks. It will benefit audit- and compliance-related activities. It will also provide customers with the necessary information to perform detailed analyses of their security environments for planning purposes and forensics in the case of a security breach.
- **Vulnerability Scanning:** This service enables the customer's IT infrastructure to be scanned on a weekly and monthly basis. It can be provided/delivered from MEEZA's facilities or even the customer's on-premises facilities.

MEEZA also provides security consulting services. MEEZA's SOC is one of the first commercially available SOCs in the Gulf States. Previously, these services were available to local customers from providers located outside of the region. MEEZA is aiming to expand its market coverage outside of Qatar by making its SOC services portfolio available throughout the Middle East.

Challenges

Customers face various challenges in information security, including, but not limited to, the adoption and implementation of information security solutions and services:

- **Complexity of IT Environments and Security-Related Tasks:** Information security solutions are deployed either as point solutions or integrated solutions, creating diverse and complex IT environments that are not easy to manage.

Adopting an SOC service will create concerns around the ownership of information on networks, as well as concerns around the type of SLA that will be agreed between the customer and the SOC provider.

- **Views on the Use of an SOC:** Many large organizations in the region tend to invest in having an in-house SOC. This is largely due to privacy concerns around their own networks and data systems. The issue of who manages incidents is a major concern, and the perception is that incidents can be better managed when the SOC is available in house.

- **Compliance and Policies Impacting Security Adoption:** The number of regulations impacting a wide range of verticals is expected to increase. The use of an SOC will create additional requirements that companies will have to ensure are in place in order to remain compliant with regulations.

Conclusion

Cybercrime is now more prevalent than ever. With the growing frequency of advanced persistent threats, the need for effective threat intelligence is extremely critical. Since attacks are being launched with the aim of causing broader political and economic repercussions, companies need to leverage their threat intelligence to better protect themselves from attacks and mitigate the damage.

In light of these developments, IDC recommends the following:-

- Companies in Qatar need to re-evaluate their current security environments and decide on either setting up their own SOC or utilizing the services of an existing one.

- If companies decide to setup their own SOC, they need to keep in mind the high level of CAPEX required not just to setup the infrastructure but the time to setup the SOC as well as finding and developing the right people with the right skill sets. People and processes are key for any successful SOC monitoring.

- When choosing to adopt security services, companies should engage with partners that can provide a holistic view of security and can ensure real time support in case of incidents. The service provider should have a team of local security professionals who are industry certified.

- Companies should approach SOC providers who are transparent about the level of security being provided and how they adhere to industry best practices and standards.

- Organizations should also evaluate the level of data and network privacy being provided by the SOC provider.

- Lastly, the SOC provider should be able to provide detailed reports at defined time intervals that can be shared by clients with their internal stakeholders.