INNOVATIVE SOLUTIONS

Whitepaper:

THE RISE OF CYBER ATTACKS AND COUNTERMEASURES

deep i™

discover it before others do!

deep
discover it before others do!

Table of **Contents**

Executive **Summary**

Spectrum of digital enhancements and innovation in the interconnected world of information technology is expanding at a very high speed. The concept of world to be a global village has become reality with **49.6%** active internet users in the world. The number of IoT devices will grow to 50 billion by 2020 and it is estimated that there will be 200 billion Internet-connected devices by 2030. The fast-paced technological innovation associated with businesses is fraught with risks. This rapid evolution is also under a constant cyber threats from malicious actors.

Cyber threats are constantly evolving, drawing executives' attention to the expansion of the threat landscape and demanding additional investment in the cybersecurity function to minimize or eradicate the impact of incidents on organizations. In 2016 alone, 18 million new malware samples were identified and more than 4000 ransomware attacks have occurred. A single breach can cause havoc to businesses, such as bringing operations to a standing halt or financial loss and reputational damage of an organization. The rising tide of cybercrime has pushed cybersecurity spending on products and services to more than $80 billion in 2016.

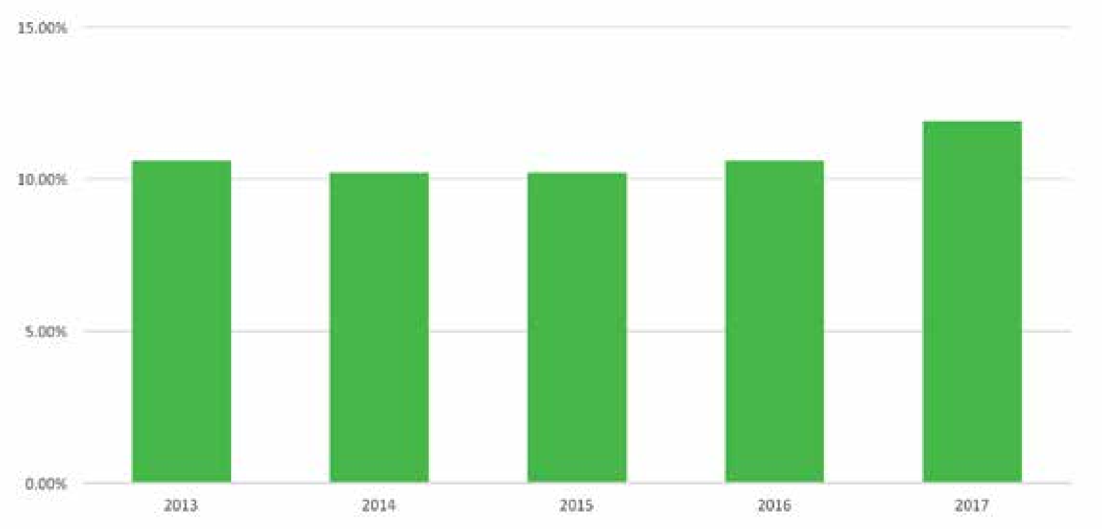
These technological advances bring challenges and pose high risks. Organizations in the Middle East especially are more prone to cyber-attacks as studies have shown. A pressing issue faced by organizations is the long time adversaries remain undetected within an environment which result in further damage to compromised systems. In addition, cybersecurity skills shortage is one of the biggest challenges facing organizations that has a significant impact on addressing security risks.

As cybersecurity becomes a complex issue for many organizations, establishing a strategic partnership with Managed Security Service Providers (MSSPs) has been a well sough after solution for maintaining robust cybersecurity operations and building reliable capabilities. Outsourcing security services allows organizations to have direct access to turnkey solutions, unparalleled threat intelligence and incident response to get better return on investments while meeting the unique demands of your business.

Introduction

Saudi Arabia's digital transformation has proven its success beyond doubt. The number of internet users in the Kingdom continues to rise rapidly, reaching about 24 million users in 2017, with massive population penetration in the Middle East of 74.9% in comparison to 48.9% worldwide. 500 government services are now offered online and technological advances are heavily utilized in all sectors to keep pace with the competitive market.

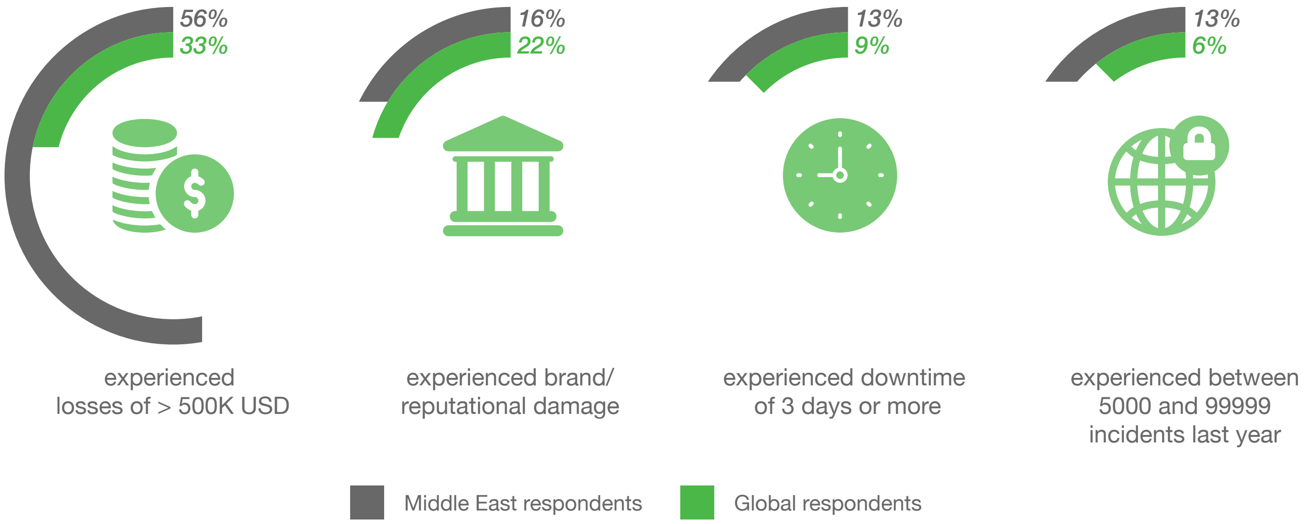
The extensive use of technology poses high risks of cyber-attacks. As the threat surface continues to expand, the potential sources and types of threats are becoming more prevalent and sophisticated. Adversaries are constantly hiking up their efforts to destabilize the region's IT advancements with cyber-attacks. In 2015, Saudi Arabia recorded over 160,000 offensive cyber actions a day, making it the most targeted country in the Middle East. Predictably, most of the targets were the Kingdom's oil and gas, banking, and telecom sectors.



Cyber threats are growing more hostile, security skills are in shortage and imperatives like mobility and cloud computing can pose additional business risks. All these factors have led to a sharp rise in investing in cyber defense capabilities to protect critical assets and sensitive information. However, not all investments have yielded the desirable results. As an alternative, establishing a strategic partnership with a competent Managed Security Service Provider (MSSP) has been a well sough after solution for maintaining robust cybersecurity operations and building reliable capabilities. Although organizations remain accountable for information security and business risks, engaging an MSSP allows to offload tactical and operational tasks and gain access to advanced skills and services. More organizations are committing to outsourcing cybersecurity functions so they can focus on mission critical skills. As shown in the graph, the percentage of total IT spending on outsourcing increased from 10.6% in 2016 to 11.9% in 2017.

Challenges & Risks

Cybersecurity is one of the biggest economic challenges countries face in the twenty-first century. The Middle East is one of the most advanced regions when it comes to the speed of technology adoption and population growth. Organizations in the Middle East are more prone to cyber threats compared to the rest of the world. As shown in the graph, around 18% of respondents in the region have experienced more than 5,000 attacks compared to a global average of only 9% ranking the Middle East higher than any other region according to PwC Survey.



One of the biggest issues faced by organizations is the prolonged detection timeframe. Adversaries gain access to compromised networks for a long time allowing the infliction of further damage, while organizations are mostly unware of malicious actors presence until it’s too late. The average time that adversaries stay undetected on a network is over 146 days according to FireEye.

Another pressing issue facing organizations is cybersecurity skills shortage which affects the ability to defend against cyber threats. In a survey by Global Information Security Workforce, it was found that in the Middle East and Africa alone, 67% of respondents admitted that cybersecurity departments are understaffed due to lack of qualified professionals.

The shortage of cybersecurity experts will be the main cause of failure to address digitized risks for almost 60% of businesses. Not surprisingly, IT security is one of the most growing field being outsourced due to the restrictions in ability to hire staff with the required skill sets.

The impact of cyber threats on organizations is huge. The cost and consequences of cyber-attacks, such as business disruption, financial losses, privacy violations, loss of customer trust and most importantly reputational damage, can be catastrophic if not dealt with strategically.

Way Forward

With booming IT in the Middle East, despite the slow pace of security capabilities growth, organizations need not only the right technology, but the right people, the right governance structures and the right processes.

Organizations need to adopt a proactive approach to identify risk and understand their impact on the business. To proactively respond to cyber threats, many organizations have resorted to different approaches such as periodic risk assessment, enforcing security policies, increasing security awareness, deploying complex defense systems and ad-hoc monitoring.

However, establishing and maturing these components is costly, time consuming and prone to failure.

One of the most reliable options adopted by many organizations around the world has been to establish strategic partnerships with Managed Security Services Providers (MSSPs) to ensure optimal protection from latest emerging threats and remediation measures before attacks proliferate.

The use of Managed Security Services (MSS) is on the rise as the market size is projected to grow from USD 17.79 Billion in 2015 to USD 35.53 Billion by 2020 with an estimated annual growth rate of 14.8% during the coming years. Furthermore, 42% of respondents in a research conducted by ESG stated they are already using an extensive set of MSS.

Benefits of engaging a **MSSP**

COST

The cost of MSS is less than hiring in-house, full-time security experts. An MSSP is capable of spreading out the investment in analysts, hardware, software, and facilities over several clients, cutting the per client cost.

STAFFING

A shortage of qualified cyber security professional puts enormous pressure on IT departments to provide adequate assurance. On the other side, service providers invest in training and retaining highly skilled security experts.

SKILLS

Unlike MSSP professionals, internal employee will have limited exposure to threats and incidents and therefore will have limited experience in detecting and handling techniques. Moreover, MSSPs have better visibility of security impacts across several different clients.

FACILITIES

Many MSSPs have special security operations centers (SOCs) located in different locations with state-of-the-art infrastructure and technologies.

ASSURANCE

A MSSP can provide an independent and objective assessment of the security posture of an organization as well as maintaining a high level or rigor through continuous evaluation.

ACCESSIBILITY

A MSSP is often able to obtain advance warning of new threats and vulnerabilities and gain early access to information on specialized countermeasures.

SERVICE PERFORMANCE

MSSP's operational procedures are designed to ensure uninterrupted service availability and real-time reporting, 24x7x365 days. MSSPs have strict obligations towards clients and are held accountable for the service standards provided.

Risks of engaging an **MSSP**

TRUST

Building trust between clients and service providers could be difficult for some organizational cultures. Decision makers might find it challenging to make the call and engage a security provider. However, this partnership needs to be recognized at an executive level.

OWNERSHIP

Accountability might be degraded as employees may start to ignore pressing security issues having delegated this concern to service providers. Establishing roles and responsibilities for information security can assist in mitigating this risk.

IMPLEMENTATION

Transitioning cyber security functions to service providers may require a complex shift for employees and organizations.

How **Innovative Solutions (IS)** can assist?

Cyber threats are growing more hostile, security skills are in shortage and imperatives like mobility and cloud computing can pose additional business risks. Innovative Solutions can help address your complex cyber security challenges, through turnkey solutions, unparalleled threat intelligence and incident response and highly flexible Managed Security Services (MSS), namely deep (i), designed to get better return on investments while meeting the unique demands of your business.

The **deep (i)** suite offers the following services:

- **deep (i) -** SOC Monitoring
- **deep (i) -** Endpoint Protection
- **deep (i) -** Incident Response
- **deep (i) -** Web Security

Managed SOC Monitoring

Real-time analysis of security posture on an ongoing basis where information systems of an organization are continuously monitored, assessed and defended.

Managed Incident Response

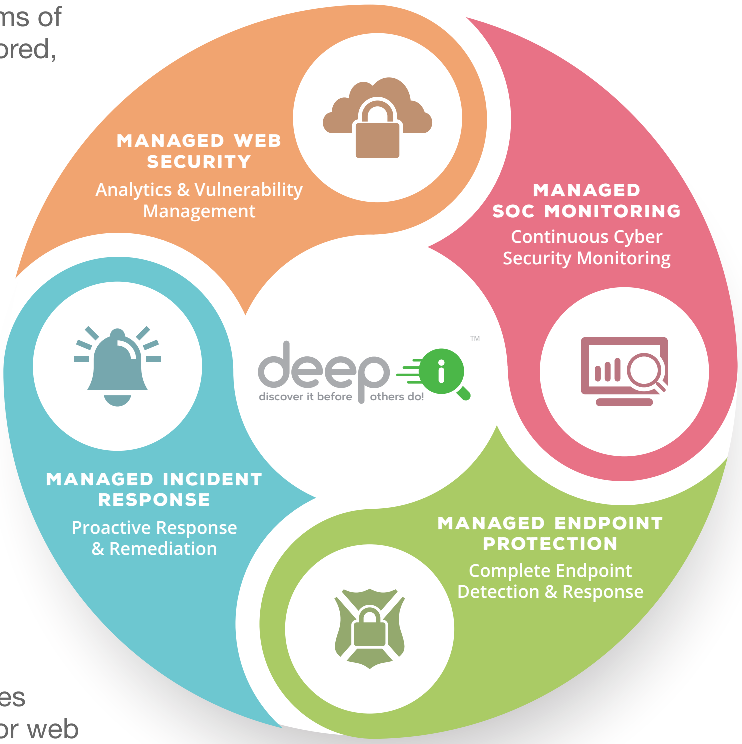
A complete state of the art managed incident response service that tracks all details of the activity occurring in the environment with complete visibility using instant Root Cause Analysis (RCA) to provide real time monitoring, prompt response and proactive remediation.

Managed Endpoint Protection

Monitoring all activities on endpoints using the most scalable application control solutions with ability to block malicious and unknown files.

Managed Web Security

An in-house developed tool that provides continuous and consistent assurance for web applications by detecting weaknesses before exploitation. The tool generates zero false-positive reports that are validated and tested (penetration testing) by our security consultants at regular intervals for accurate results.


MANAGED WEB SECURITY
Analytics & Vulnerability Management
MANAGED SOC MONITORING
Continuous Cyber Security Monitoring
MANAGED INCIDENT RESPONSE
Proactive Response & Remediation
MANAGED ENDPOINT PROTECTION
Complete Endpoint Detection & Response
deep i
discover it before others do!
TM

INNOVATIVE
SOLUTIONS

Head Office

P. O. Box 69328, Riyadh 11547,
Saudi Arabia

+ 966 11 2931501

info@is.com.sa

www.is.com.sa

Branches

Dubai | Jeddah | Al Khobar

@Innovative-Solutions

@is_arabia

Innovative Solutions SA