Aldar Audit Bureau
Abdullah Al-Basri & Co.
Member firm of Grant Thornton International Ltd.
Grant Thornton

Action

Cybercrime

Respond and restore

Navigating cyber crime during a crisis

grantthornton.sa

#RespondandRestore #Cybercrime

> “Cyber-attacks are more focused, skillful, and ambitious. Regulators and stakeholders are increasing the pressure on organisations to manage these risks.”
>
> **Abdullah Al-Basri, Managing Partner**
> **Aldar Audit Bureau – Grant Thornton**
> **Kingdom of Saudi Arabia**

Foreword

As organisations become increasingly dependent on digital technology, the opportunities for cyber criminals continue to grow.

The annual global cost of cyber crime is estimated to reach $6 trn by 2021 as attacks increase in quantity and sophistication annually[1].

The surge in data generated by digital technology, combined with a new degree of connectedness among organisations and individuals, means that there is ripe opportunity for the technologically savvy and criminally minded taking advantage.

Cyber attacks are more focused, skillful, and ambitious. Geographical borders are meaningless. Regulators and stakeholders are increasing the pressure on organisations to manage these risks, hence cyber security is now a priority in boardrooms, specifically during times of crisis.

Whilst global spending on security-related hardware, software and services will grow at a compound annual growth rate (CAGR) of 9.2% between 2018 and 2022, to a total of $133.8 bn in 2022[2], organisations will still be exposed to risk as the prevalence of cybercriminals increases, specifically as the crime is often quick and difficult to trace.

As businesses increasingly expand their online presence in the wake of the crisis, the exposure of their client base will also increase. It is estimated that over 2bn people who have used online services have had their data stolen[3]. Such exposure will deter online consumers, hampering e-commerce sales, unless businesses can mitigate risks through effective strategies.

Closer to home, the Kingdom of Saudi Arabia (KSA or Saudi Arabia) has recently been identified as one of the top countries who have been the most effected by ransomware, followed by Turkey and China[4]. In order to manage this trend, companies across Saudi Arabia are urged to employee professionals or attract talent who have expert cyber-skills in order to manage and mitigate risk.

As the Kingdom continues to progress towards its Vision2030 ambition, the need to increase capability and knowledge of cyber crime will become prominent, particularly as the exposure of such risk will continue to rise year-on-year, which will have a crippling effect on businesses, stakeholders and its consumers.

Abdullah M. Al-Basri
Managing Partner
Aldar Audit Bureau - Grant Thornton, Saudi Arabia

Contents

Annual global cost of cybercrime is estimated to reach **$6trn by 2021.**

$3.25bn global revenue was generated by social media-enabled crimes.

Post-data breach responses cost businesses **$1.43mn** in the Middle East.

[1] Cybercrime damages 6 trillion by 2021, Cybersecurity Ventures
[2] Global Security Spend Set to Grow to $133.8 Billion by 2022: IDC, Security Week 2019
[3] Economic Impact of Cybercrime: No Slowing Down, McAfee, 2018
[4] Cyber threat defense report, Cyber Edge Group, 2019

The global view

The global annual cost of cyber crime is estimated to reach $6 trn by 2021 as cyber-attacks increase in quantity and sophistication[1]. The significant financial and reputational damage caused by such crimes must act as an alert for business owners and key stakeholders, who need to have a proactive approach to building cyber defences.

We depict the global impact to illustrate the severity of the crime.

- Up to 0.80% of the world's GDP is now being lost to cyber crime.
- Though it constitutes a relatively new criminal economy, cyber crime is already generating at least $1.5trn in revenues annually.
- $3.25bn global revenue is generated by social media-enabled crimes. [5]

The industry view

- Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%.[6]
- 15% of breaches involved Healthcare organisations, 10% in the Financial Services sector and 16% in the Public Sector.[7]
- Smaller organisations (1–250 employees) have the highest targeted malicious email rate at 1 in 323.[8]
- Lifestyle (15%) and Entertainment (7%) were the most frequently seen categories of malicious apps.[8]

Security spending

- The United States and the Middle East spend the most on post-data breach response, with the U.S. spending $1.56 mn and the Middle East having spent $1.43 mn.[9]
- 50% of large enterprises (with over 10,000 employees) are spending $1 mn or more annually on security, with 43% spending $250,000 to $999,999, and just 7% spending under $250,000.[10]

Cyber security roles

- It is predicted that by 2021, 100% of large global companies will have a CISO position.[11]
- By 2021, it is projected that there will be 3.5mn unfilled cybersecurity roles.[12]
- Since 2016, the demand for Data Protection Officers (DPOs) has risen over 700%, due to the GDPR demands.[9]

Globally, cybercrime threats continue to increase at an exponential rate, with specific industries being more prone to attacks, due to the value of data which they possess. Whilst cybercrime has increased as a priority across boardrooms, the ongoing challenge of access to talent and increased security funding will hold businesses back from defending themselves effectively.

[5] 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends, Comparitech 2020
[6] Data Risk Report, Varonis 2019
[7] Data Breach Investigations Report, Verizon 2019
[8] Internet Security Threat Report, Symantec 2019
[9] Cost of Data Breach Study, Ponemon Institute 2017
[10] Big Security in a Small Business World, Cisco 2020
[11] Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, Cybercrime magazine 2019
[12] Rise of the data protection officer, the hottest tech ticket in town, Reuters 2018

> Whatever your sector, whatever type of business you are, assume that you are being targeted all the time. With the levels of volume cyber crime, we are seeing now, you almost certainly are.”

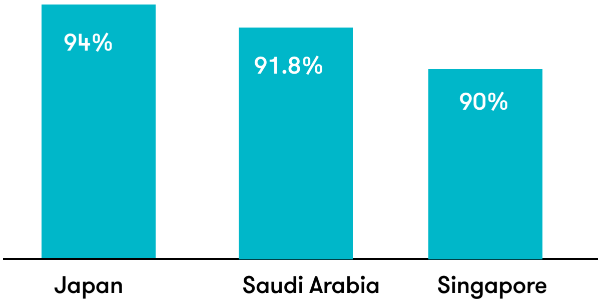
James Arthur
Partner and Head of Cyber Consulting
Grant Thornton UK

The view from Saudi Arabia

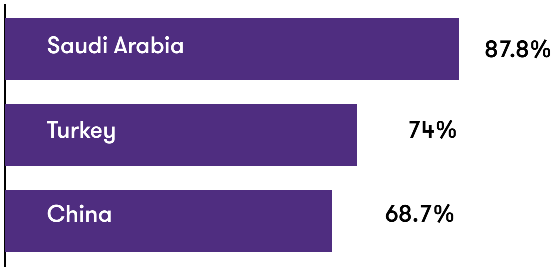
Revenue generation in the cyber crime economy takes place at a variety of levels – from large 'multinational' operations that can generate profits of over $1 bn; to smaller scale operations, where profits of $30,000- $50,000 are more the norm. Given the diverse market profile of businesses based in Saudi Arabia, businesses are both targets and vulnerable to such threats.

Leaders across Saudi Arabia are urged to safeguard their valuable assets which include people, data and systems.

In 2019, Japan, Saudi Arabia and Singapore were impacted by a shortage in cyber security skills.[9]



Saudi Arabia, along with Turkey and China were the most affected by ransomware [9]



> “Cyber crimes have increased during this pandemic due to phishing techniques disguised under COVID-19 related texts or emails containing viruses. Awareness is the first line of defense against cybercrimes and then comes using secured networks (including VPNs) through stronger firewalls and hardware like data diodes. This pandemic has convinced the market for a paradigm shift towards digitalisation.”
>
> **Umair Butt, CFO**
> **Jubail Water and Power Company**

Canada and Japan allocate 4% of their security budget to technology, followed by Saudi Arabia who invest 2.8%, which is relative to market size. That said, the three countries which have displayed the fastest growing technology security budget include Turkey (7.1%), Brazil (6.8%) and China (5.8%).[9]

In response to its Vision2030 strategy, Saudi Arabia will continue to invest in its national transformation program, which will be powered by technology and hence we predict that security investment will continue to increase in correlation to the countries ambition.

Following on from the United States, Saudi Arabia has been ranked second in the cost of data breaches, with 38,800 number of compromised records per breach, compared to the global average of 25,575.[9]

The commercial landscape is changing rapidly, with the volume of data generated growing exponentially. Businesses across Saudi Arabia are encouraged to identify their data and technology vunlnerabilities in order to build mitigating strategies to protect the organisations reputation and value.

> “Cyber security risks have increased dramatically due to businesses being unprepared and rapidly shifting to adopt the new norm. With single access, malware or viruses can go through the VPN and compromise the entire company’s network. We urge businesses to consider adopting effective strategies to mitigate such risks.”

Ahmad Al Zoubi, Director, Advisory
Aldar Audit Bureau - Grant Thornton, Saudi Arabia

Mitigating risk and managing cyber crime

No organisation or industry is immune to cyber-crime.

As cyber-attacks dominate the headlines, regulators and stakeholders are under increasing pressure to manage cyber risk. There is more to managing digital risk than relying on technology alone, therefore businesses must adopt several non-tech measures to protect themselves.

Develop a strategy

Leaders will have to step into the shoes of cyber criminals, understand the threats these groups pose and develop proactive strategies to protect their business' interests whilst addressing their digital vulnerabilities.

Have the right structure

Internal governance, processes and people are important aspects to consider, along with ensuring the right structure is developed and adopted. Additionally, we recommend businesses undertake a structured programme to assess and validate their most valuable data assets, using a categorisation and classification process, enabling them to invest in appropriate insurance cover.

Manage trust and reputation

Businesses must understand the value they deliver to the customer, once this has crystallised, the potential impact a breach would have on the relationship can be formed, enabling effective mitigating strategies to be adopted. Businesses should consider customer relationship managers and trust policies to correlate with the technology being used.

Educate your people

To enable its people to understand and manage risks effectively, we recommend developing shorter, more frequently distributed training videos and simulated phishing attempts, along with ensuring skilled resources are available across the business to support ongoing development.

Recruit specialised resources

Specialised cyber skills are required, therefore we recommend having access to resources who can complement cyber security technical skills with commercial acumen. This will ensure that your investment in preventive software is focused in the right areas, along with having an additional safeguard for stakeholders and the business to rely on.

Insure yourself effectively

Which email threads could a former employee leak to embarrass their former managers? What intellectual property and trade secrets would be of interest to a foreign power? And how might a cyber-criminal use your data to try to extort money from your business? These are just some of the questions you need to ask before purchasing insurance as part of your digital risk management plan.

> “Cyber resilience is crucial in developing business resilience. I believe this is the time to review, test, and update the Business Continuity Plan to ensure that it is up-to-date and copes with post-COVID 19 demands. There is going to be a huge shift in operating models as the market culture is changing towards remote working.”
>
> **Nawaf Al Habdan, Risk Officer**
> **Yamama Cement**

Key pillars for your cyber risk management plan[13]

1. The increasing amount of data customers share with brands means that trust is more important than ever. It is essential that businesses understand the necessity of trust management, and that digital risk policies and procedures go a long way to ensuring this.

2. Traditional approaches to cyber training are not working. Businesses should develop shorter, more frequently distributed training videos and simulate phishing attempts to better educate their workforces.

3. Businesses need to identify and map out their digital vulnerabilities. They need to recruit staff with specialised cyber skills that complement cyber security technical skills. This will ensure that their investment in preventive software is focused on the right areas.

4. The risk of suffering a cyber-attack is prominent– no matter how much is invested in preventive software. Investing in insurance can bolster your risk management, but it is crucial to insure your most valuable data assets and explore specific insurance that covers both cyber- attacks and data-privacy breaches. Once insurance is secured, businesses must be vigilant about adhering to the terms and conditions. If they fail to install updates, it could nullify the insurance.

These recommendations must be implemented in the context of businesses' specific digital risk environments. The first step for business leaders is to understand their vulnerabilities and threats. Only then can they implement the most relevant technologies, training initiatives and insurance coverage.

> “Globally, cyber crime threats continue to increase at an exponential rate. It is imperative that businesses develop strategies to mitigate the risk in order to effectively manage the new emerging phase.”

Imad Adileh, Principal
Aldar Audit Bureau - Grant Thornton, Saudi Arabia

[13] Grant Thornton UK, Digital Risk is no silv er bullet

Cyber laws in Saudi Arabia

Practical advice for businesses.

> "Cyber crime and cybersecurity legislation is developing rapidly around the world. The recent global trend has seen governments and regulators introducing new laws or tightening existing legislation to impose more stringent cybersecurity obligations on organisations."

Dino Wilkinson, Partner
Clyde & Co

While technological developments have helped many organisations to increase efficiency through digitisation of records and processes, the changes have also increased their vulnerability to cyber threats as more aspects of business are conducted electronically. Corporate IT systems (and the data they hold) are vulnerable to a range of threats including criminal organisations, disgruntled clients, ex-employees, activists and cyber terrorists.

As a result, cyber crime and cybersecurity legislation is developing rapidly around the world. The recent global trend has seen governments and regulators introducing new laws or tightening existing legislation to impose more stringent cybersecurity obligations on organisations and higher penalties on cyber criminals.

At an international level, examples include the introduction in Europe of the General Data Protection Regulation (GDPR), the Network & Information Security Directive and the Cybersecurity Act. These new pieces of legislation substantially increase the scope of organisations that will be subject to European cybersecurity laws, potentially including all businesses established in or providing services into the EU. The GDPR, in particular, introduced strict new rules on data security, reporting and breach notification with potential fines for non-compliance of up to €20 mn or 4% of annual global turnover (whichever is greater).

Overview of cyber regulation in KSA

The Government of the Kingdom of Saudi Arabia (KSA) has stated in the Saudi Vision 2030 a clear intention to diversify the national economy through a strong focus on digital transformation.

The need to establish a safe online environment for individuals, enterprises and government has driven a substantial amount of legal and regulatory development in recent years.

The Anti-Cyber Crimes Law was issued back in 2007 and remains the basis for establishing cyber offences in the

Kingdom. It criminalises both a range of technology-enabled offences (such as defamation or invasion of privacy using technological means) and crimes against IT systems (including unlawful access or interception of data).

The Communications and Information Technology Commission (CITC) in its role as the information and communications technology (ICT) sector regulator in KSA has more recently issued regulations incorporating specific cyber and data security obligations on ICT providers. These include:

- the Information Security Policies and Procedures Development Framework for Government Agencies, which was developed by the Computer Emergency Response Team – Saudi Arabia (CERT-SA) to provide a framework for government entities to develop their information security procedures;
- the Cloud Computing Regulatory Framework, which establishes rights and obligations for both cloud service providers and cloud customers, including specific information security, content classification and data localisation requirements; and
- the Internet of Things (IoT) Regulatory Framework, which was published in 2019 and includes data security requirements that apply to IoT providers and implementers.

In 2017, the National Cybersecurity Authority (NCA) was established to further strengthen national information security with a mandate to regulate cybersecurity matters in the Kingdom. The NCA issued the Essential Cybersecurity Controls in 2018 and has published a draft set of Cloud Cybersecurity Controls for public consultation in early 2020. Both sets of controls are intended to mitigate cybersecurity risks for the country by applying standards to be followed by KSA government entities and providers or operators of critical national infrastructure.

There are also regulations that apply to businesses in certain regulated sectors. The Saudi Arabian Monetary Authority (SAMA) has a Cybersecurity Framework that was published in 2017 and sets out a minimum set of information governance standards and controls for banks, insurance companies and other financial institutions.

Practical tips

All organisations operating in KSA should understand the legal and regulatory landscape applicable to their business operations in order to be aware of cybersecurity compliance obligations. They should also be taking steps to understand their level of vulnerability to cyber risk by considering their organisational structure, data processing activities and potential threats. An audit of this nature should also identify where data or systems are shared with other parties and the controls that are in place.

Subsequent risk management measures might include the implementation of standard policies for staff and/or suppliers, reviewing contract documentation and ensuring that appropriate information is given to individual employees and customers about the use of their personal data.

Staff should be suitably trained to identify and manage cyber risks, which should include an understanding of the legal and regulatory landscape specific to the business and the type of data it holds. It is becoming increasingly important for all companies to have an incident response plan ready to implement in the event of a cyber attack and many organisations are further mitigating risk through cyber insurance coverage.

About Clyde & Co

Clyde & Co is a dynamic, rapidly expanding global law firm focused on providing a complete legal service to clients in our core sectors. Clyde & Co's global team provides a market leading end-to-end cyber solution, tailored to your needs. For further information, please visit www.clydeco.com

Supporting you to manage your cyber-exposure

Our team of local experts can support businesses to manage their forensic and cyber-exposure through our proven methodology, which includes:

Prepare

We help you understand your current exposure to cyber security risk and support you to develop an effective security capability. Our services include cyber security risk and threat assessments; security policy development; security -process or technical assessments; and third-party cyber security assurance.

Protect

We develop and implement the technical framework and broader processes required to protect. We can help you with security architecture; security technology implementations; security process design and implementation; identity and access management; privacy and data protection; data classification; enterprise application integrity; business continuity and disaster recovery; and penetration testing.

React

We work with you to support and monitor your cyber security operations and help you to respond rapidly and forensically in the event of a security or data breach.

Change

We can help you improve and better manage your cyber security capability. Our services include security programme strategy and planning, security governance; and security awareness.

Contact our professionals to find out more

Imad Adileh
Principal
iadileh@sa.gt.com

Ahmad Al Zoubi
Director
aalzoubi@sa.gt.com

Contributors:

Dino Wilkinson, Partner, Clyde & Co.

Umair Butt, CFO, Jubail Water and Power Company

Nawaf Al Habdan, Risk Officer, Yamama Cement

All statistics as referenced, were correct at the time of publishing.

About Grant Thornton

Aldar Audit Bureau, Abdullah Al-Basri & Co. ('Grant Thornton Saudi Arabia'), is a member firm of Grant Thornton International Ltd. As one of the world's leading accounting and consulting firms we offer comprehensive assurance, tax and specialist advisory services to privately held businesses and public interest entities who span across a wide range of industries.

With over 30 years of experience in Saudi Arabia, we understand the needs of businesses who are dynamic, having worked with clients who range in size and industry. Our personalised local approach coupled with our global reach makes Grant Thornton Saudi Arabia the ideal advisers for organisations that are ambitious and who want to go beyond.

Visit **grantthornton.sa** today to find out how we can help you.

Riyadh
Al Mousa Commercial Complex
7th Floor, Tower 4
Al Olaya Street, Riyadh
T +966 (11) 463 0680

Jeddah
Saad H. Abu Khadra Building
3rd Floor, King Fahad Street
Jeddah 21455
T +966 (12) 691 6883

Dammam
Ababtain Tower
7th Floor, Dhahran Street
Al-Khobar, Dammam
T+966 92 000 6582

Aldar Audit Bureau
Abdullah Al-Basri & Co.
Member firm of Grant Thornton International Ltd.
Grant Thornton

grantthornton.sa

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.