شـركة وادي الرياض
Riyadh Valley Co

Cybersecurity Industry
Global Protection against Cybercrime

November 2020

Cybersecurity and its importance

What are cyberattacks?

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's system/network.

Common types of cyberattacks

Malware breaches a network through a vulnerability, when a user clicks a dangerous link or email attachment that then installs risky software.

Malware

Ransomware
A type of malware that blocks access to key components of the system/network.

A type of malware that covertly obtains information by transmitting data from the hard drive.

Spyware

Phishing
Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth.

Denial of service attack

Botnets
These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities.

What is Cybersecurity?

Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access.
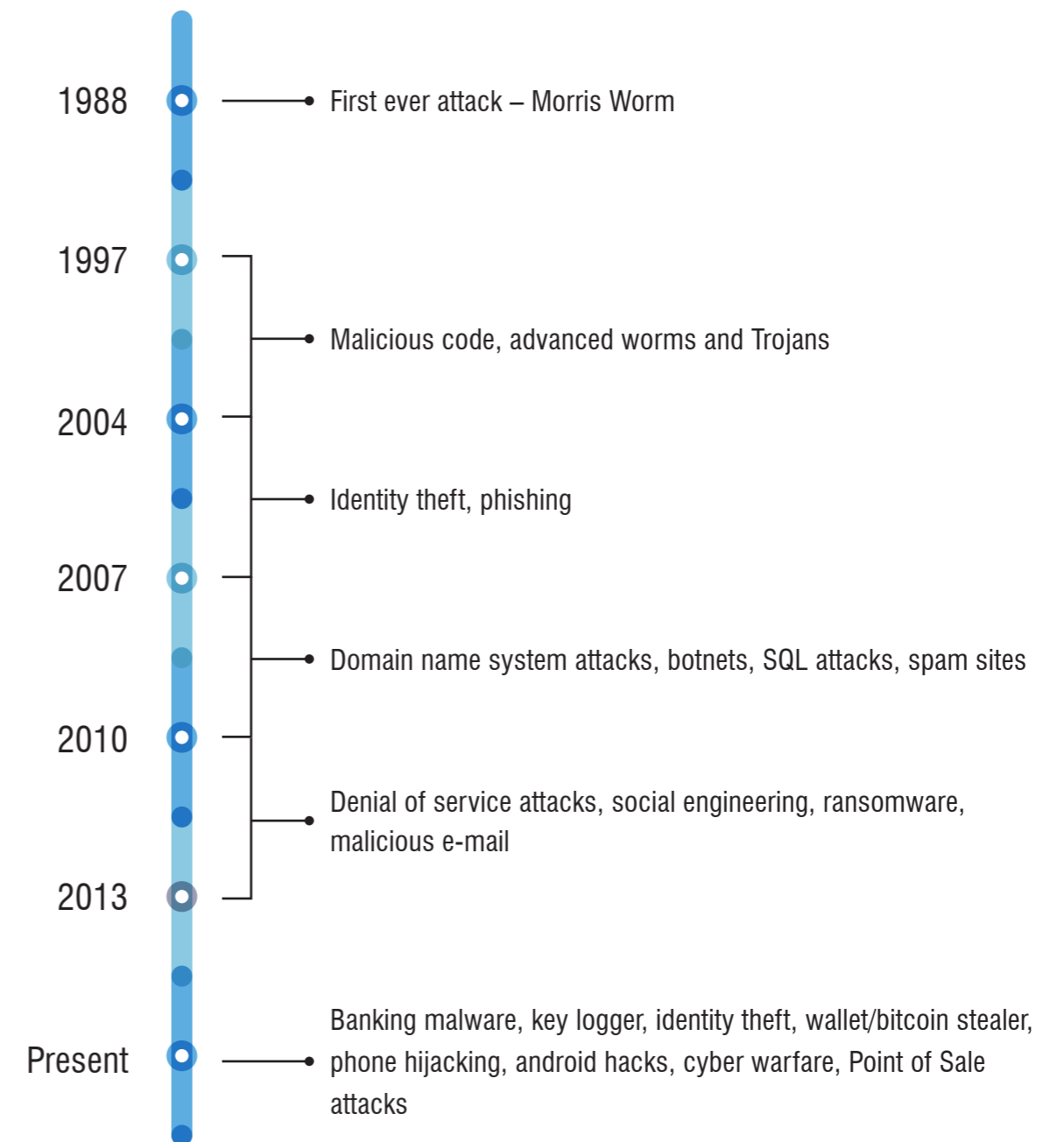
Why is Cybersecurity important?

Governments, corporations, and people have moved to digital means of storing data in recent years. As they collect, process, and store vast amounts of confidential information and transmit that data across networks, cybersecurity has become more important in the current digital age.

Source: Cisco, NASDAQ

Complexity of cyber-attacks have increased over the years
Evolution of Cyberattacks

Year	Event
1988	First ever attack – Morris Worm
1997	Malicious code, advanced worms and Trojans
2004	Identity theft, phishing
2007	Domain name system attacks, botnets, SQL attacks, spam sites
2010	Denial of service attacks, social engineering, ransomware, malicious e-mail
2013	
Present	Banking malware, key logger, identity theft, wallet/bitcoin stealer, phone hijacking, android hacks, cyber warfare, Point of Sale attacks

Source: Infosec

**Every industry is prone to cyber-attacks in different ways**

Security incidents matrix by industry and attack type – 2019

Industry	Crimeware	Web Applications	Privilege Misuse	Denial of Service	Cyber Espionage	Lost and Stolen Assets	Point of Sale	Payment Card Skimmers	Miscellaneous Errors	Everything Else
Accommodation	19%	16%	1%	0%	1%	4%	45%	0%	6%	8%
Education	8%	8%	5%	59%	2%	2%	0%	0%	10%	6%
Finance	6%	8%	11%	62%	3%	1%	0%	2%	4%	3%
Healthcare	16%	15%	23%	1%	1%	13%	0%	0%	22%	8%
Information	19%	7%	1%	62%	2%	0%	0%	0%	6%	2%
Manufacturing	16%	11%	10%	46%	5%	1%	0%	0%	4%	6%
Professional	9%	12%	2%	61%	1%	2%	0%	0%	4%	9%
Public	20%	0%	56%	4%	1%	12%	0%	0%	6%	0%
Retail	9%	39%	7%	23%	1%	3%	4%	4%	5%	6%

Source: Verizon, Nasdaq

Banking and Utilities sectors have the highest average cost of cybercrime

Average annual cost of cybercrime by industry (USD Mn.)


■ 2018   ■ 2017
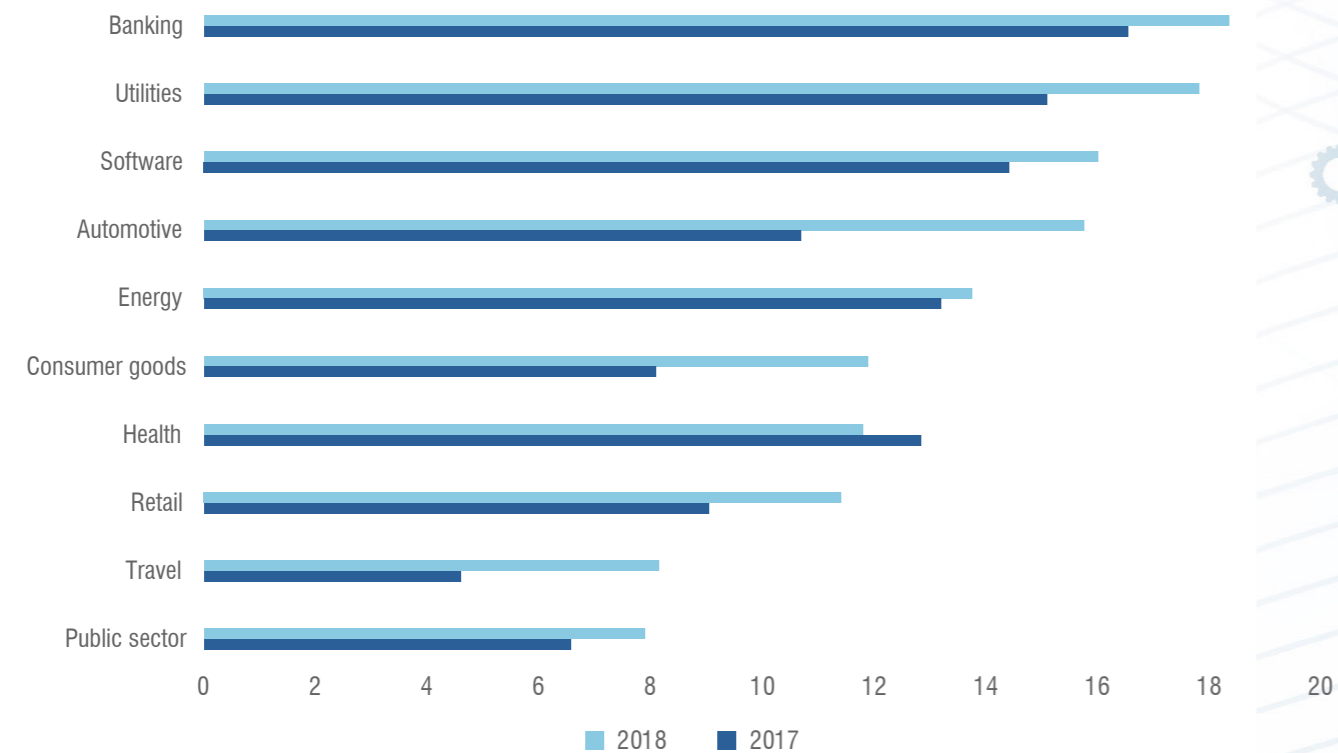
Source: Accenture; Note: Cost of cybercrime includes the cost incurred to detect, recover, investigate and manage the malicious incident response. It also includes the cost of efforts to reduce business disruption and the loss of customers.

Cybersecurity Market Overview

**Middle East and Africa's cybersecurity market expected to grow significantly in 2021**

Global cybersecurity market by geography (USD Bn.)

Legend: Middle East, Latin America, Asia Pacific, Europe, North America
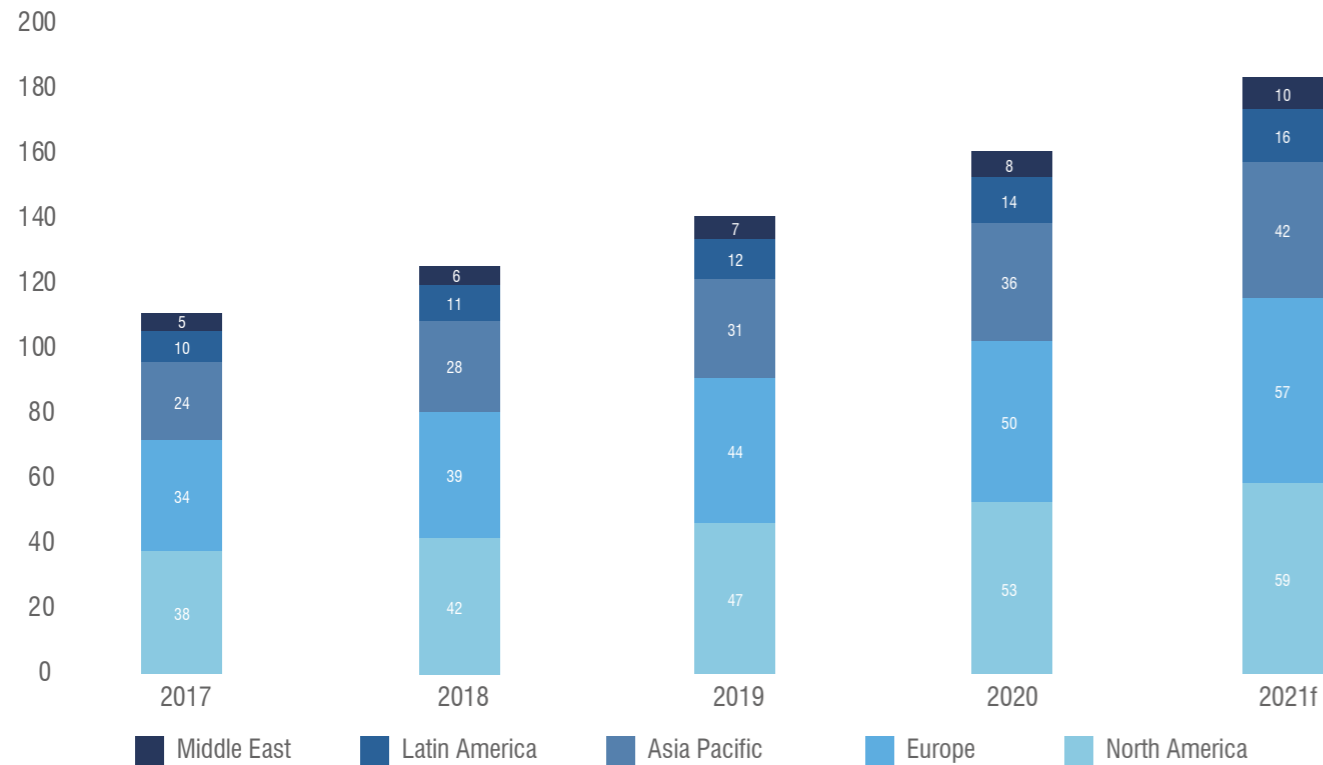
Source: Technavio, KPMG

Government cybersecurity installations have seen a notable increase in the past few years

Global cybersecurity market by sector (USD Bn.)

Legend: Others, Healthcare, Retail, ICT, Manufacturing, BFSI, Government
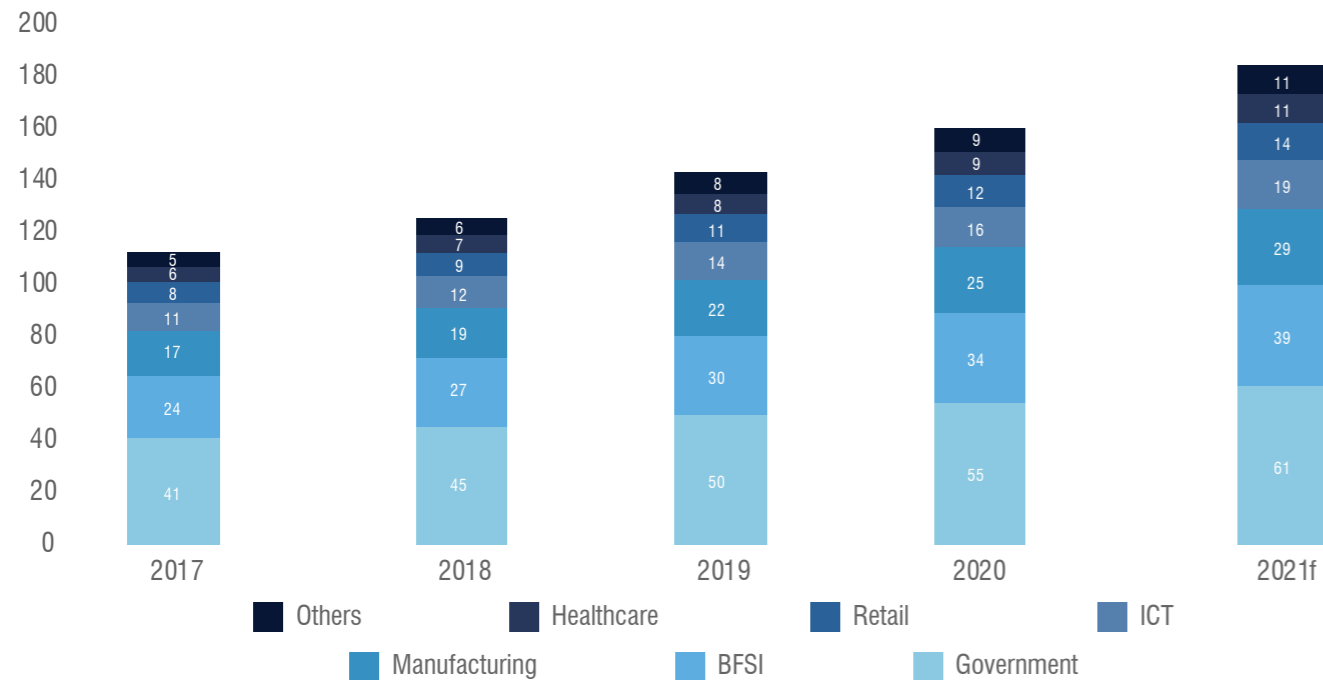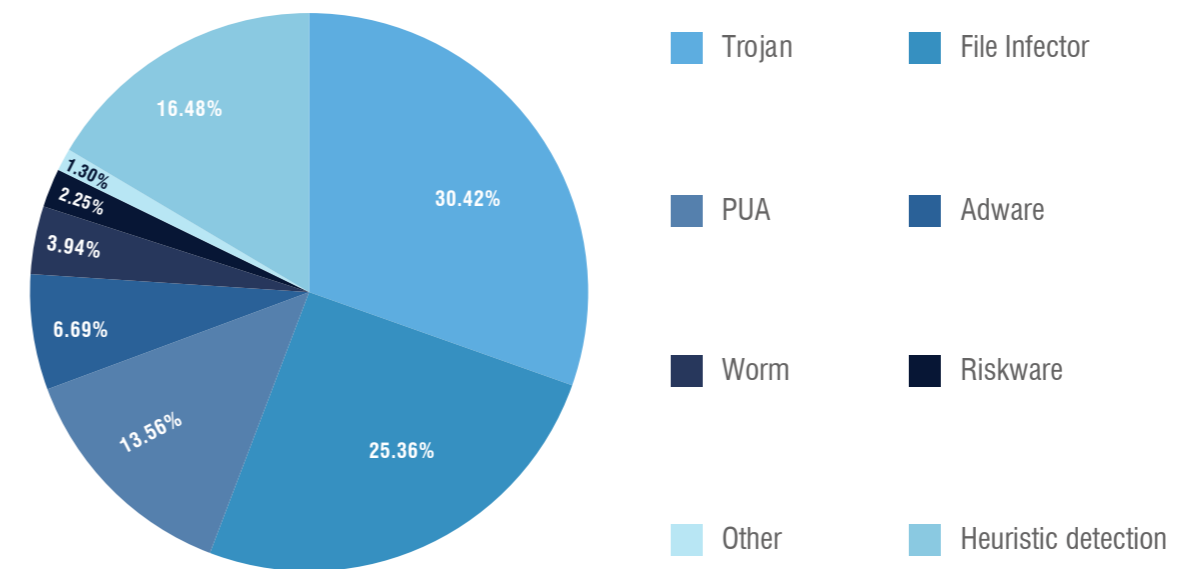
Source: Technavio, KPMG

Types of Cyberattacks

Portable Executable (PE) attacks

PE is used to describe binary executables files within the Windows OS that usually have the file format '.exe' or '.dll'. Security threats arising from malware that are disguised as these PE files are known as PE attacks.
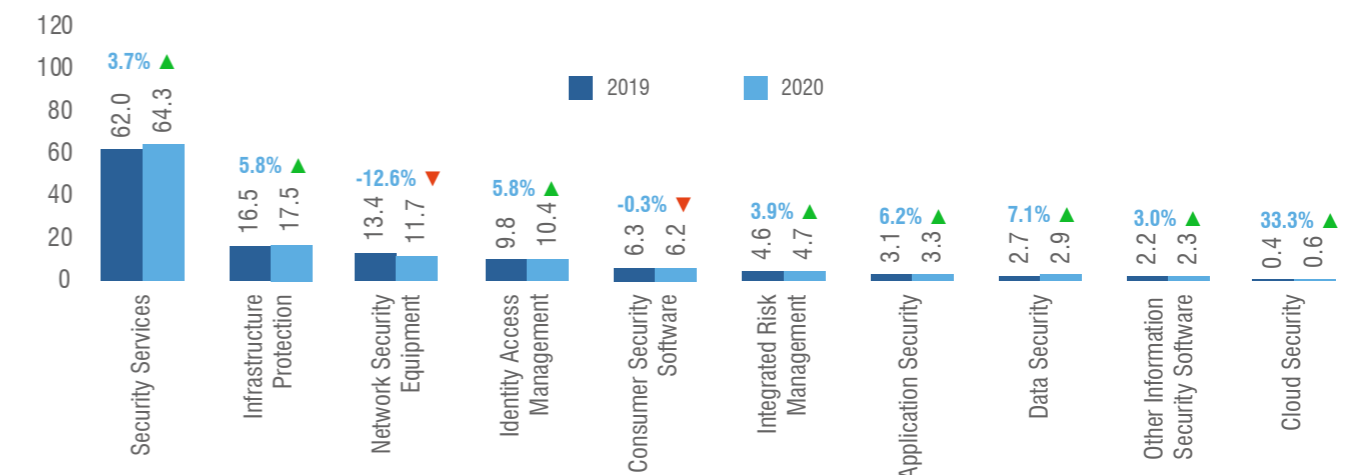
Non-PE attacks

Non-PE threats are a means of infecting machines without the use of executable files. The attacking mechanism will be through Office files, scripts, PDFs, and other exploits.

Type of PE Malware threats (Q2 2020)

Pie chart values: 30.42%, 25.36%, 13.56%, 6.69%, 3.94%, 2.25%, 1.30%, 16.48%

Legend: Trojan, File Infector, PUA, Adware, Worm, Riskware, Other, Heuristic detection

Source: Avira malware threat report - Q2 2020; Note: PUA - Potentially Unwanted Application

Global Cyber Security Spending by segment (USD Bn.)

Legend: 2019, 2020

Segment	2019	2020	Change
Security Services	62.0	64.3	3.7% ▲
Infrastructure Protection	16.5	17.5	5.8% ▲
Network Security Equipment	13.4	11.7	-12.6% ▼
Identity Access Management	9.8	10.4	5.8% ▲
Consumer Security Software	6.3	6.2	-0.3% ▼
Integrated Risk Management	4.6	4.7	3.9% ▲
Application Security	3.1	3.3	6.2% ▲
Data Security	2.7	2.9	7.1% ▲
Other Information Security Software	2.2	2.3	3.0% ▲
Cloud Security	0.4	0.6	33.3% ▲

Source: Gartner (June 2020)

Global cybersecurity players are spending aggressively on Research and Development

Company	Symantec	Palo Alto Networks	McAfee	Trend Micro	FireEye
Revenue -2019 (USD Mn.)	4,731	2,900	2,635	1,578	889
R&D expenses -2019 (USD Mn.)	913	540	380	79	271
Year of establishment	1982	2005	1968	1988	2004
Headquarters	USA	USA	USA	Japan	USA
Major Clients	• AIG • The Economist • Budapest Bank	• Accenture • IBM • Google Cloud	• Microsoft • SanDisk • Toshiba	• Amazon Web Services • Cisco • Oracle	• Vodafone • QNB Finansbank • Bank of Thailand

Source: KISLine, CapitalIQ, Company Data, KPMG; Note: R&D - Research and Development

Cybersecurity in KSA

Saudi Arabia's Cybersecurity market expected to nearly double in size by 2023 compared to 2019

Saudi Cybersecurity Market Size (USD Bn.)
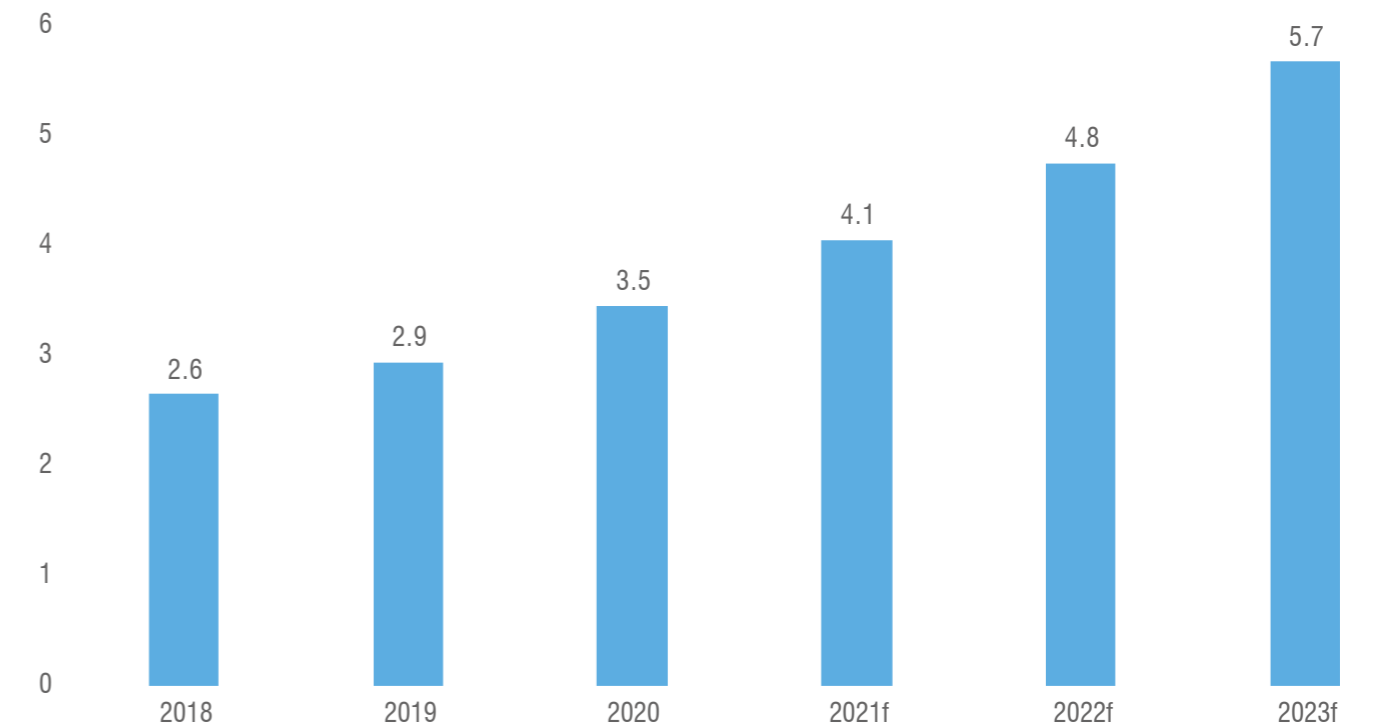
Source: 6W Research, USSABC estimates

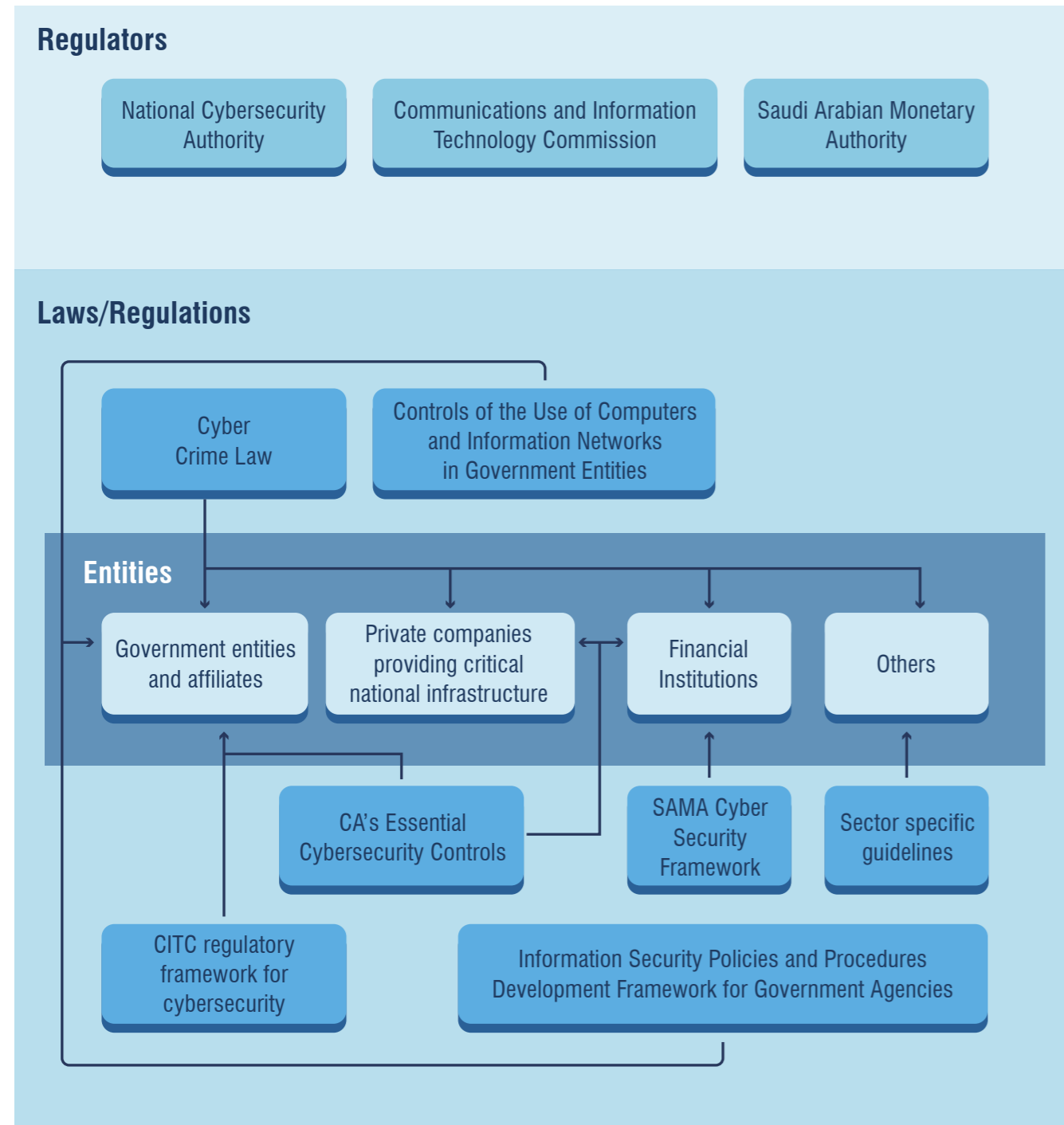**Saudi Arabia ranks first among MENA countries in global cybersecurity rankings**

Global Cybersecurity Index rankings

Country	Global Rank - 2018	Global Rank - 2017	Change in Rank	
Saudi Arabia	**13**	**46**	▲	**33**
Oman	16	4	▼	-12
Qatar	23	14	▼	-9
UAE	33	47	▲	14
Kuwait	67	139	▲	72
Bahrain	68	65	▼	-3

Source: ITU - Global Cybersecurity Index

SAMA established a Cyber Security Framework to enable Financial Institutions to effectively identify and address risks related to cyber security.

Saudi Arabia Cybersecurity regulatory landscape

Regulators

| National Cybersecurity Authority | Communications and Information Technology Commission | Saudi Arabian Monetary Authority |

Laws/Regulations

| Cyber Crime Law | Controls of the Use of Computers and Information Networks in Government Entities |

Entities

| Government entities and affiliates | Private companies providing critical national infrastructure | Financial Institutions | Others |

| CA's Essential Cybersecurity Controls | SAMA Cyber Security Framework | Sector specific guidelines |

| CITC regulatory framework for cybersecurity | Information Security Policies and Procedures Development Framework for Government Agencies |

Source: Regulatory authorities' websites, Simmons & Simmons

Saudi-based companies are expected to ramp up investments in cloud security

Saudi Arabia's Enterprise Cybersecurity Spending Forecast (USD Mn.)

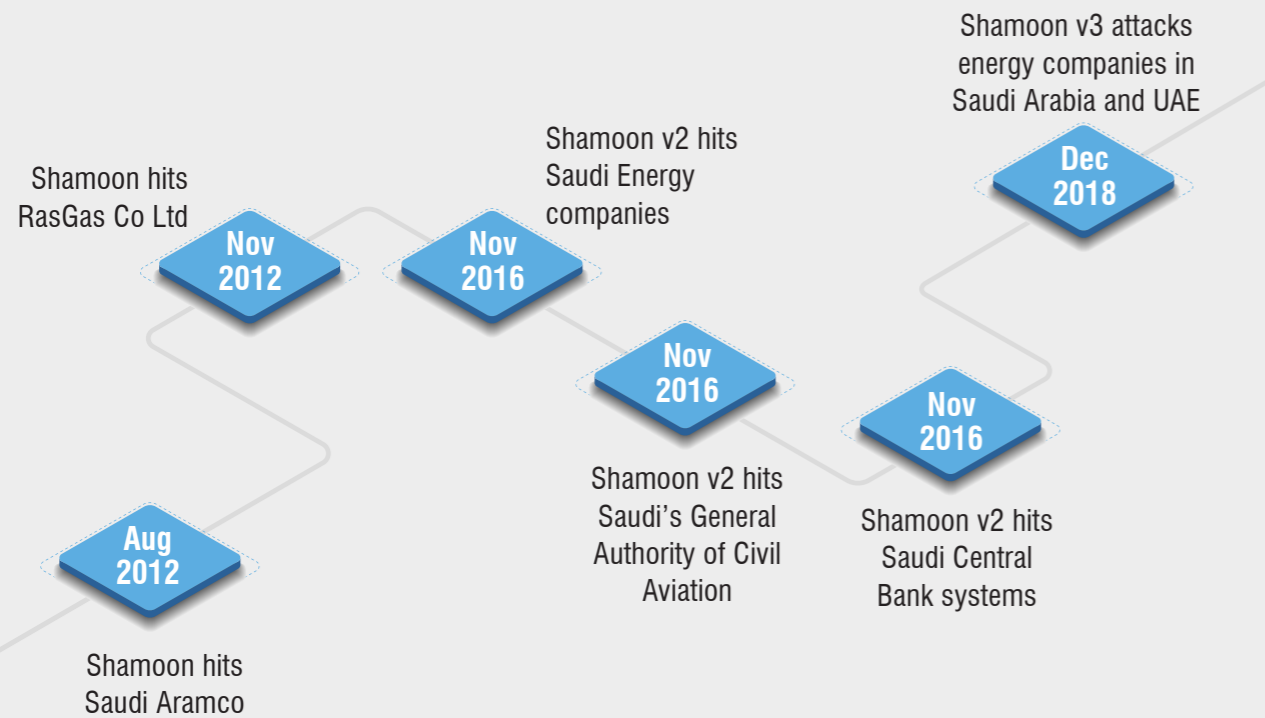| Market	2018	2019	2020	2021f	2022f	2023f	CAGR
Application Security	6	7	7	8	9	10	10.6%
Cloud Security	1	1	2	4	6	9	53.4%
Consumer Security Software	23	25	27	29	31	33	7.6%
Data Security	7	8	11	14	17	20	23.6%
Identity Access Management	25	28	33	39	43	48	13.4%
Infrastructure Protection	26	31	35	41	47	53	14.8%
Integrated Risk Management	4	5	6	8	9	10	20.4%
Network Security Equipment	45	53	58	64	67	70	9.4%
Other Information Security Software	4	4	4	4	4	4	0.0%
Security Services	104	116	127	138	151	163	9.4%
Total	**246**	**278**	**311**	**348**	**385**	**420**	**11.3%**

Source: Gartner, USSABC

Several SMEs remain vulnerable and have no understanding of protecting themselves from cyberattacks

Establishments targeted by cyber attacks in Saudi Arabia

Sector	SMEs	Large Firms	Total
Retail	432,106	3,811	**435,917**
Finance, Real Estate, and Insurance	39,735	1,130	**40,865**
Education	6,074	3,253	**9,327**
Healthcare	2,411	1,749	**4,160**

Source: GAStat

Case Study - Shamoon attacks

Shamoon v3 attacks energy companies in Saudi Arabia and UAE

Dec 2018

Shamoon v2 hits Saudi Energy companies

Nov 2016

Shamoon hits RasGas Co Ltd

Nov 2012

Nov 2016

Nov 2016

Aug 2012

Shamoon v2 hits Saudi's General Authority of Civil Aviation

Shamoon v2 hits Saudi Central Bank systems

Shamoon hits Saudi Aramco

Source: Blackberry

Key Highlights

- On August 15, 2012, a destructive malware named Shamoon attacked the computer systems of Saudi Aramco. The attack was planned at a time when nearly 55,000 employees stayed home from work. It resulted in 30,000 or more systems being damaged.

- Shamoon is an information-stealing malware, which also included a destructive module.

- Shamoon renders infected systems unusable by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once a system is infected, it attempts to spread itself to other devices on the local network.

- The malware re-emerged in November 2016 as Shamoon 2. The attack campaign brought three waves of destructive attacks to organizations within Saudi Arabia.

- Again after a two-year absence, the destructive malware Shamoon re-emerged on December 10, 2018. Symantec found evidence of attacks against a few organizations in Saudi Arabia and the UAE.

Spotlight: Seculetter

SECU LETTER

SecuLetter is a cybersecurity service company that provides cutting-edge solutions to detect unknown attacks with hybrid approaches. The company aims to be a global leader in security industry by leveraging their technology that is more advanced than existing security systems.

Headquarters: Seongnam, Gyeonggi, South Korea

Founded: 2015

SecuLetter success in preventing Shamoon attacks

- Using its capability, SecuLetter will be able to identify cyberattacks such as Shamoon that have re-emerged across the Middle East region.

Key Highlights

- SecuLetter is one of Riyadh Valley Company's investment portfolio companies.

- SecuLetter's solution detects and diagnoses non-PE files that cannot be checked with normal behaviour based diagnostic techniques.

- SecuLetter's solution executes reverse engineering to check the characteristics of malicious files coming through e-mail and analyzes the file at assembly level so that the system does not wait until there is any malicious activity.

- While professional analysts can analyze approximately 20 malicious codes a day, SecuLetter's solution including automated technique of professional analysts is able to process about 180,000 malicious codes a day.

SecuLetter' s product offerings

| Product Name	SLE (SecuLetter Email)	SLF (SecuLetter FileServer)
Products Description	It is a specialized threat analysis protection solution for email. SLE is able to block cyberattack, which uses malicious code passing over the weakness of email security.	It is a specialized threat analysis protection solution for Fileserver. SLF is able to block the attack via attachment which targets organization that shares files server for co-work.
Features	• Analyses malicious code attached in email. • Checks malicious code in file downloaded through the link in email content. • Sends an alarm to administrator about email verified as malicious code, and resends it by setting. • Provides detailed report of the malicious code detection result.	• Diagnoses and blocks malicious code of the file coming into internal network. • Diagnoses malicious code infection history of the file in storage. • File check without capacity limit. • Provides administrator alarm and intuitive management report after malicious code detection.

شـركة وادي الريـاض
Riyadh Valley Co

Riyadh Valley Company

Riyadh Valley Company established in 2010 by Royal Decree No.116 dated 13/4/1431 AH to be the investment arm of King Saud University in the fields of Knowledge Economy and the university strategic projects.
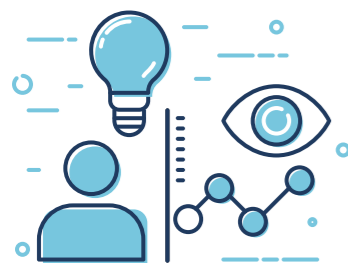
Vision

To be the regional leader in knowledge-based investment and technology.

Mission

Riyadh Valley Company is a strategic investor, focused on leveraging the local capabilities, investing locally and globally in growth - stage businesses to create financial and strategic returns that will support the future of economic development in the Kingdom.
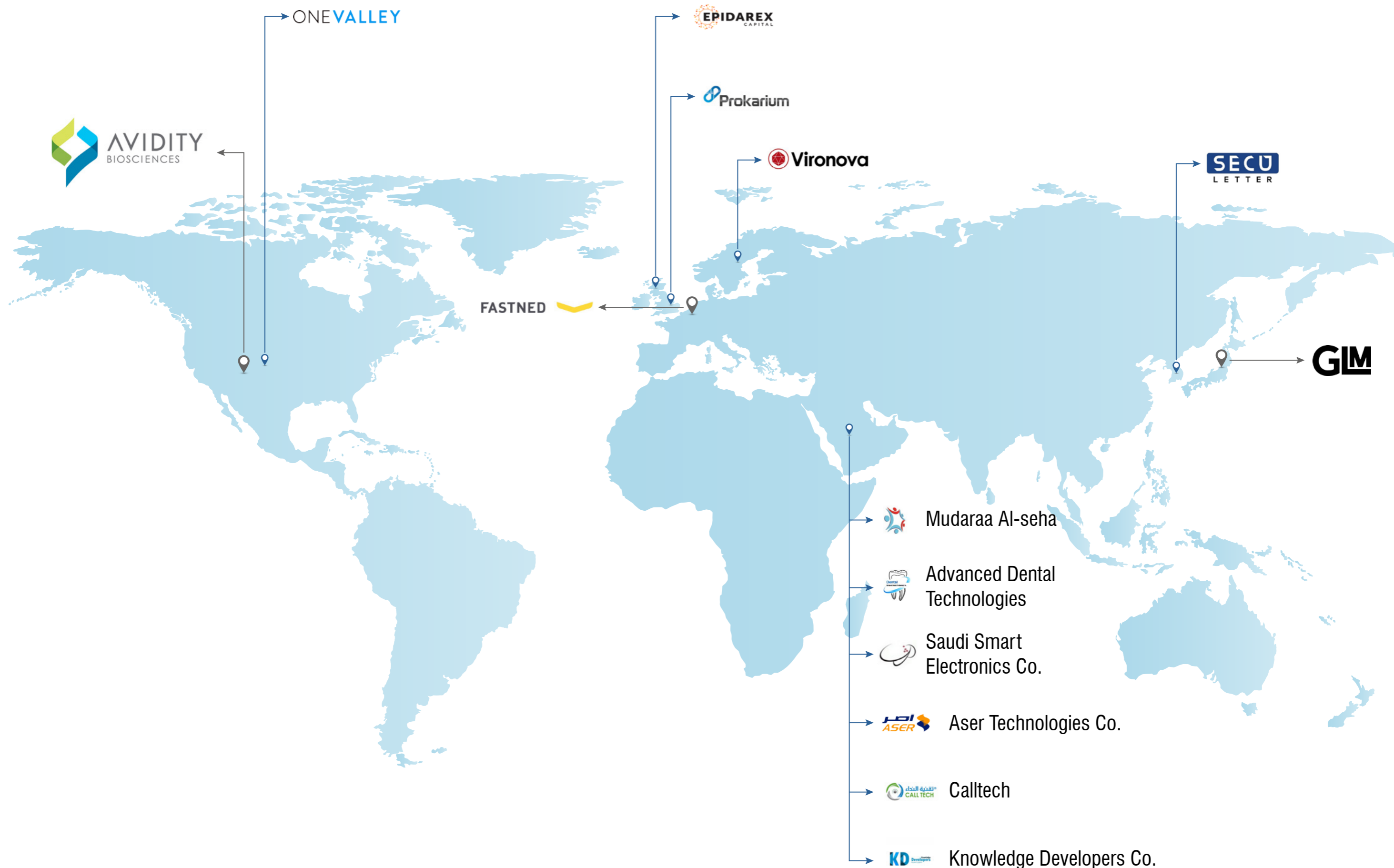
Investment Sectors:

Knowledge Investments

- Healthcare investment
- Renewable energy& sustainable recourses
- Information & Communication technology

Real Estate Investments

- Innovation and R&D Projects
- Commercial Projects
- Educational Projects
- Residential Projects
- Healthcare Projects
- Mixed-use Projects

Knowledge Investment Portfolio

ONEVALLEY

EPIDAREX CAPITAL

Prokarium

AVIDITY BIOSCIENCES

Vironova

SECU LETTER

FASTNED

GLM

Mudaraa Al-seha

Advanced Dental Technologies

Saudi Smart Electronics Co.

ASER Aser Technologies Co.

CALL TECH Calltech

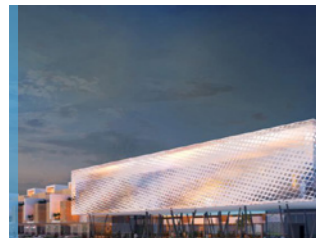KD Knowledge Developers Co.

Real Estates Investment portfolio

Sudair Pharma Company Project

Research center and company offices for Sudair Pharma Company

ELM Information Security Company Project

Innovation Center project for Elm information security company

Al-sorooh Al-Mubarakah Company Project

Mixed-use project contains office complex, Mall, Restaurants, cafes, and walkway for visitors

Obeikan Company Project

Commercial project contains various stores near the Common First Year building

Four Directions Company Project

Commercial and office project contains office buildings and multi-use halls

Retail Real Estate Company Project

Social-Entertaining and sports project

Derma Clinic Company Project

Medical-Commercial project contains several medical clinics, medical products stores, and pharmacies

Dur Alkuttab Company Project

Educational project for Primary Schools

Derma Clinic Company Project (Residential)

Residential project for Derma Medical Clinics

City Lights Real Estate Company Project

Entertainment-Commercial project contains screens on the building and architectural blocks, in addition to areas for live shows

Arrowad For Higher Education Company Project

Educational complex, Arrowad colleges University campus in Riyadh

Omnia Real Estate Development Company Project

Commercial project contains various shops

NMR Real Estate Company Project

Mixed-use project includes a hotel, restaurants and cafes

Hamad Bin Mohammed Bin Saedan & Partners Investment Company Project

The project serves King Saud University Campus residents. It includes large areas where events that reflect Saudi culture are held

Unified Real Estate Development Project

Cultural-Entertainment project that includes Luxury restaurants, Cafes, Cinemas and green spaces

University Boulevard

Commercial-Entertainment project gives visitors a different experience, and it includes Restaurants and cafes

Sahat Al-Ardh Company Project

A commercial project contains various shops

Riyadh Valley Company

Kingdom of Saudi Arabia, Riyadh – King Saud University, Innovation Tower

+96611 469 3219 | **www.rvc.com.sa** | info@rvc.com.sa

🐦 @riyadhvalley   in Riyadh Valley Company (RVC)