THE OPEN DIGITAL ENVIRONMENT OF THE internet is widely viewed as anarchic, dangerous and confusing, a place former US National Security Agency and CIA Director Michael Hayden once referred to as a "global free-fire zone." It is easy to feel overwhelmed and outgunned by tenacious and ingenious adversaries – criminals, hacktivists and even nation states. That wildness is set to increase dramatically.

The fourth industrial revolution is well under way. In 2017, the Internet of Things harbored approximately 18 billion connected devices; the total is expected to stand at 75 billion by 2025, a fourfold increase. Keeping pace with that growth, new cyber threats have emerged for consumers, businesses and financial institutions around the world.

To meet these challenges, the cybersecurity industry as a whole is also changing. New companies such as DarkMatter have emerged to find solutions to the evolving threats. As a younger company, DarkMatter approaches the problems from a more holistic perspective.

"I feel the industry's current approach to cybersecurity has been overly reliant on perimeter security and reaction to threats," says DarkMatter Founder and Managing Director Faisal Al Bannai. "This has ironically left entities more vulnerable to attack. Companies are investing in the equivalent of a Maginot Line when what we need is to encourage the use of evolving ecosystems designed to respond to the relevant attack.

"Walls haven't worked as defensive measures. That is very clear. Our aim is to help organizations become cyber resilient."

CYBER

BEYOND THE WALL

The Middle East is a cybersecurity hotspot. DarkMatter Founder **FAISAL AL BANNAI** tells Brunswick's **WILL ANDERSON** and **JOHN GREENWAY** about his firm's fresh approach

Founded in 2014 and based in Abu Dhabi, DarkMatter naturally sees cybersecurity with a greater urgency than companies in the West. The Middle East has seen explosive growth in its digital economy, a boom that has exposed it to a rash of cyber attacks. Fast-growing benefits and equally fast-growing threats are prompting innovative ways of weaving cyber defenses and awareness more closely and effectively into a company's DNA.

"Many locals from the emirates have grown up in a relatively safe environment but now face a situation where multiple threats are emerging online," Mr. Al Bannai says. "That's where the need for companies like DarkMatter and our concept of cyber resilience have grown from. Cyber resilience can mean having the ability to not only recover quickly from cyber attacks, but to end up stronger."

In addition to its own advisory services DarkMatter recently debuted its first product: Katim ("silence" in Arabic) is a smartphone that the company claims is the most secure mobile device made, and it markets the phone to governments and businesses in the banking sector and the oil and gas industry. The Katim is outfitted with a custom operating system, and mobile device management and productivity apps.

The company has grown rapidly, recruiting an international bench of talent that, together with its government connections, have caused some to speculate it may be involved in surveillance. Mr. Al Bannai has emphatically denied such interpretations in media reports and believes the company and the sector are aggressively headed in the opposite direction.

"As an industry, we need to establish institutional trust and transparency as pre-conditions to achieving the correct level of cyber resilience," Mr. Al Bannai says. "We often talk publicly about the need for an overarching 'Dome of Trust and Transparency' for our industry, so that we can gain access to new markets."

Cultivating that atmosphere of trust requires cooperation across the cybersecurity industry, Mr. Al Bannai says. "For an emerging industry like ours, it's imperative that we have an industry-wide platform that allows organizations to conduct comprehensive reviews of hardware and software before their installation. Those ideas remain in their infancy, but I don't think it'll take a seismic shift for them to attain wider acceptance.

"To begin rebuilding trust, developers and technology suppliers need to become more transparent about the capabilities of their products. That's a central component of the way we run our business, integral to the way we've grown in such a short timespan. But I'm also acutely aware that there's more to do to convince the general public on the big issues we face around cybersecurity."

As part of that effort, the company produced a "Cyber Resilience and Trust Report" with Brunswick Insight at the start of 2018. For Mr. Al Bannai, the report's findings reveal not just the wider trends in cybersecurity and perceptions around digital safety, but also an outline for how his business will grow over the next five years.

Included in the report's recommendations are the need for cybersecurity functions in business and government to gain organizational visibility and relevance, while developing a greater commitment to investment in software and talent. For instance, only 36 percent of cybersecurity professionals surveyed in the report responded that they currently have a direct reporting line to the CEO.

But for DarkMatter, cyber resilience is more than a concern of any one specific company; it extends to the entire community.

"We have a role to play in the wider protection of the local populace," Mr. Al Bannai says. "The scale of our Smart City program in the UAE will be vast. The cities here are growing and, with so many entry points, it's essential that we surround those cities with an evolving system of security."

Globally, cybersecurity breaches in 2017 had some major effects that have become headline news: 1.5 terabytes of data were stolen from HBO; 145 million customers of Equifax, the credit reporting service, had personal and financial data stolen; and the WannaCry ransomware attack infected systems in 74 countries worldwide.

ILLUSTRATION: NOMA BAR

The Middle East's share of that activity has grown even more dramatically. Statistics released by Dubai Police in 2017 indicated that cyber crime in the UAE increased by 136 percent between 2013 and 2015, amounting to a reported total of $22.3 million in damages and lost revenue. Across the wider Middle East, companies also suffered larger losses last year as a result of cyber incidents, compared to other regions: 56 percent lost more than $500,000 compared to 33 percent globally. Among businesses in the Middle East, 85 percent are more likely to have suffered an attack compared to the global average of 79 percent.

"The region has definitely taken great strides to improve performance, but as the Middle East continues to rapidly digitize in line with other parts of the world, hackers are finding greater opportunities to exploit vulnerabilities," Mr. Al Bannai says. "And companies have suffered larger losses than corresponding areas around the globe. There's still more that the region needs to do to ensure that it's on par with other countries around the world, but I also believe we can be at the forefront of the next global tech invention.

"One of the problems we see is that customers are often trying to find a silver bullet to solve their security issues. That's the biggest misconception we are trying to address. This is a systemic problem and you can't solve these issues unless you have a holistic approach to security."

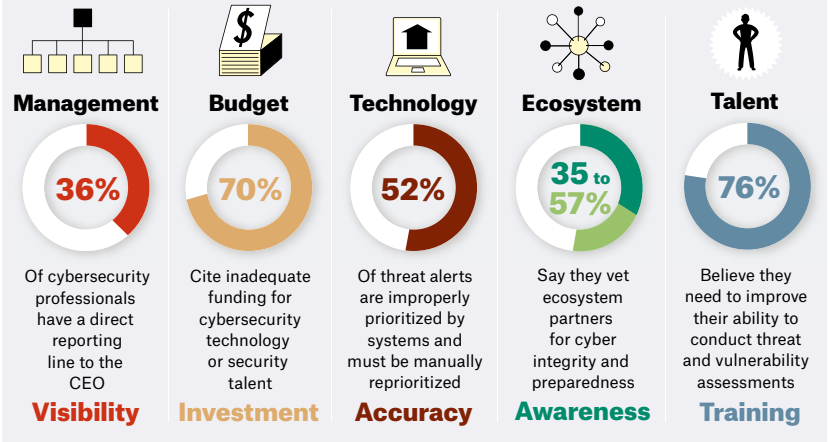
WILL ANDERSON is a Partner and the Head of Brunswick's Abu Dhabi office. **JOHN GREENWAY** is an Associate with the firm in Abu Dhabi.

DARKMATTER

A digital defense and cybersecurity consultancy and implementation firm, DarkMatter has head offices in the UAE, and research and development centers in Canada, Finland and China. Employing established, international cybersecurity specialists, the company helps safeguard the operations of large organizations, critical infrastructure and nations.

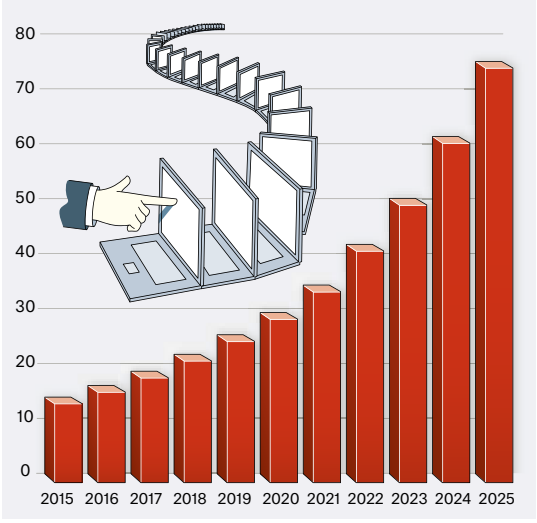
PROFESSIONALS' CONFIDENCE

The result of a survey of cybersecurity professionals by Brunswick shows some of the areas where organizations are weakest in overall cyber readiness. Most significant are perceptions of a general lack of appropriate funding and training.



EXPANDING VULNERABILITY

In 2017, DarkMatter, working with Brunswick Insight, released the "Cyber Resilience and Trust Report," using research and survey data to detail trends in data security. The chart below shows the exponential rise of Internet of Things devices – an explosive growth in connectivity that opens vast new battlefields in the international cyber war. The new vulnerabilities created highlight the need for a deeper approach to cybersecurity.

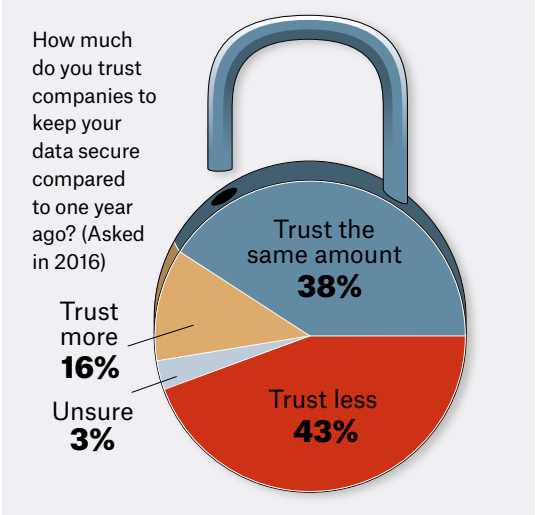


IOT DEVICES (BILLIONS)

Source: Brunswick Insight

TRUST DECLINE

Perhaps the most challenging damage as a result of cyber attack is reputational. As headlines report incidents of exposed personal consumer and customer data, fewer people consider their information safe. Brunswick Insight's survey results from 2016, below, show a marked drop in public trust.



CHARTS: PETER HOEY