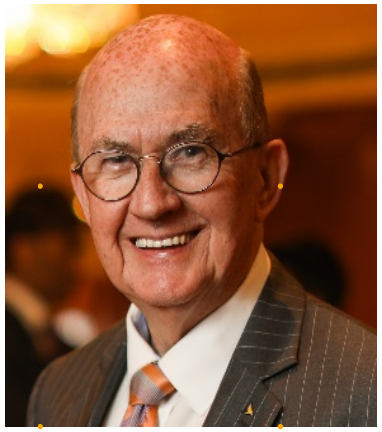


David Cafferty
Director – Risk Consulting

David Cafferty is a professional with over 30 years of experience in a variety of roles, including management and consulting in forensic accounting, financial crime, cyber crime, corporate governance, regulatory compliance and anti-money laundering for both private and public sector organisations locally, in the MENA Region, and internationally.

David heads our Regulatory Compliance and Insurance Teams with a broad profile of clients from across a variety of industrial sectors.

.

An Introduction to Cyber Crime and Cyber Security

Presented by,

David Cafferty
Director – Risk Consulting
Crowe

What is Cyber Crime?

- Cybercrime now ranks as one of the world's top four economic crimes

- Exploitation of the speed and anonymity
- Examples include:
  - attacks against computer data and systems
  - denial of service
  - identity theft
  - internet fraud
  - viruses
  - email scams

- Global nature / connectivity allows criminals
- Activities from anywhere in the world
- A new form of warfare?

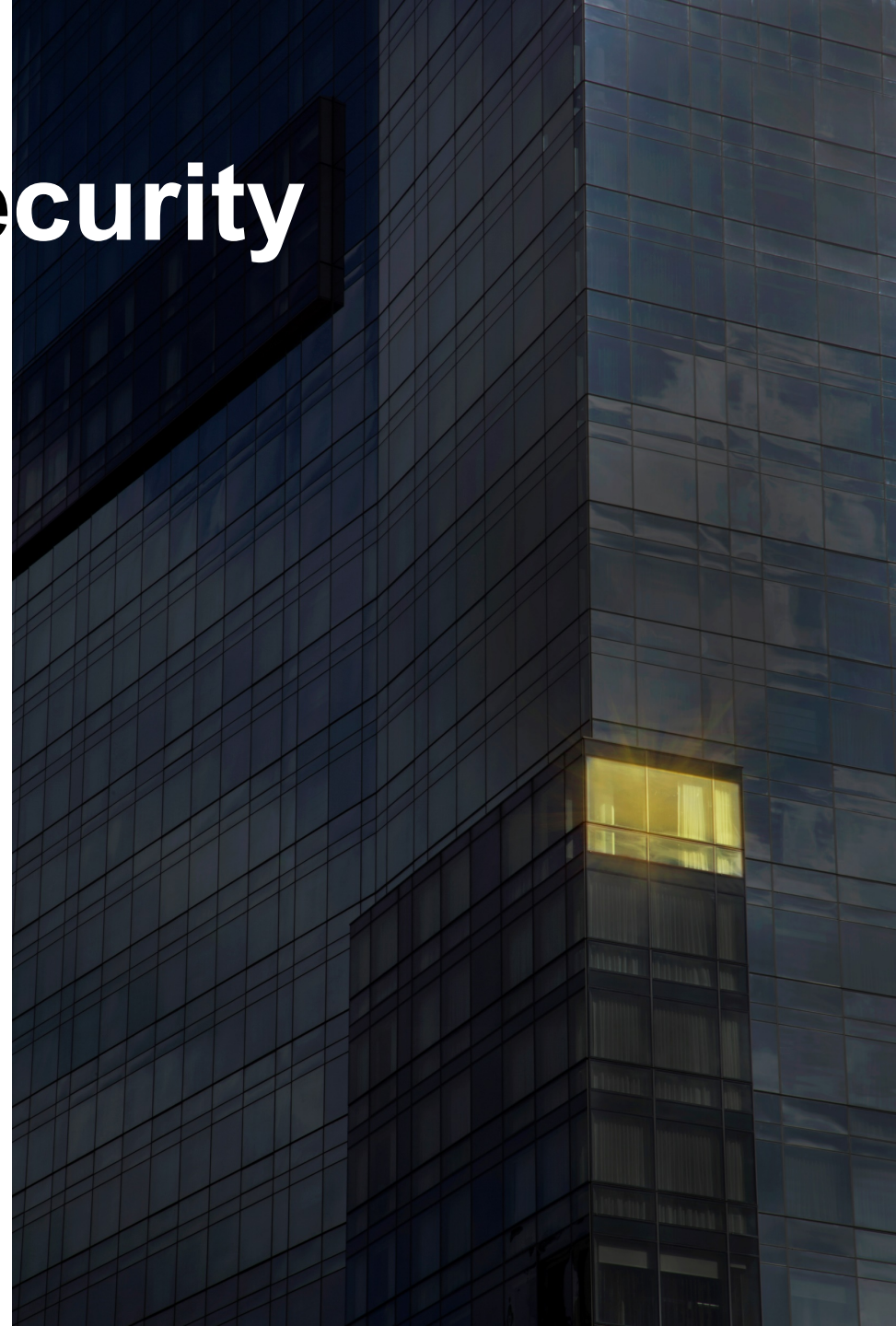
Cybercrime and Cybersecurity

- BAE Systems Detica has published a report that suggests that the biggest single issue this year was the rise of digital criminality
- Cyber-enabled financial fraud seen as the cutting-edge financial crime
- Convergence of cyber-crime and fraud the major threat
- 75% of respondents to a Cybercrime Survey of Fortune 500 company executives admitted to reporting a security breach in the last year
- Attacking mobile devices is seen as becoming the new “normal”
- Increasing trends towards cyber sabotage, with attackers seeking to have a direct effect on organisations and critical infrastructure
- Cyber-enabled identity theft and cyber-enabled theft of customer data are also increasing
- Also increasing is the threat of legal and regulatory sanctions

Cybercrime and Cybersecurity

Major attacks include:-

- British Airways
- Yahoo
- On-line stores
- Spotify
- HSBC Turkey
- J P Morgan Chase
- Microsoft vulnerabilities
- Apple IOS vulnerabilities
- “Shellshock”
- “Heartbleed”
- “Dridex”
- Careem



Common types of Cyber Attacks

TYPE	*%*
Viruses, malware, worms, trojans	50%
Criminal insider	33%
Theft of data-bearing devices	28%
SQL injection	28%
Phishing	22%
Web-based attacks	17%
Social engineering	17%
Other	11%

Regional Events

Have you been a victim?

According to a Global Economic Crime Survey, cybercrime is the second most common form of economic crime reported in The Middle East. Almost 40% of financial sector respondents were victims of cyber crimes.

Regional Cyber Crime Reports

- GCC: Qatar, the UAE and other countries in the Middle East remain among the top 10 most targeted sites in the world by cyber criminals (Gulf Times)
- UAE: Number of people reporting cyber crimes has almost doubled in Dubai (Gulf News)
- KSA: Saudi Arabia a hot target for cyber criminals (Saudi Gazette)
- UAE: Dubai Police social media accounts hacked (The National)
- MENA: Microsoft says disrupts cybercrime rings with roots in Kuwait, Algeria (Reuters)
- Qatar – Q-CERT: “whilst it is difficult to measure the actual level of financial cybercrime in Qatar, it is evident that it is on the rise here”

Disclosed Cyber Incidents in the UAE

- A cyber-attack on Dubai-based ride sharing platform Careem has resulted in the theft of personal data of up to 14 million people in the Middle East.
- Sharjah Police arrested a Pakistani national believed to be behind a $545,000 (AED2m) scam to sell Bitcoins.
- More than one million UAE consumers were victims of online shopping scams alone in 2017.
  - Losses total of AED 321 million.
  - More than one in four (22%) had their financial details.
  - 28% experience credit or debit card fraud.
  - 43% were notified their personal or financial information was compromised in a data breach last year.
  - E-commerce in the UAE is projected to be worth $10 billion by 2018.
- The average total cost of a data breach in KSA and the UAE combined is $5.31 million, a 7.1% increase since 2017.
- Global average was only $3.86 million, putting the Middle East second to the US, with an average of $7.91 million, in terms of cost of breaches.
- In KSA and the UAE, a study found that breaches cost companies $163 per lost or stolen record on average, compared to $148 globally.

Cyber Incidents in the UAE

- Average time to identify a data breach in the region is 260 days, and the average time to contain a data breach once identified is 91 days, compared to a global average of 197 and 69 days respectively.
- 10% annual growth in Cyber Insurance (Abu Dhabi National Insurance Company).
- MENA - 94% of companies admitted they have suffered a cyber-attack in the past year.
  - Real number may be even higher as not all companies admit they had breaches.
- UAE was the number one target in the region last year for spear phishing, in which attackers target specific individuals or companies. Globally, the UAE ranks eighth in such attacks.
- UAE was fourth most impacted country by crypto ransomware in the Middle East and Africa and 34th globally.
- MENA is however seen as the only geographical region which has not come under sustained attack.

The Dark Web

The Dark Web

What is the "Dark Web"?

The Dark Web, is World Wide Web Content (a series of "darknets") that can only be accessed by using specific software, configurations or authorisation to access. It forms a small part of the deep web, the part of the Web not indexed by the usual web search engines.

The Darknets which constitute the Dark Web includes small, peer-to-peer networks, as well as large popular networks, like Tor, I2P and Ripple operated by public organisations and individuals.

Why should you be concerned?

The Dark Web is well known for being a market place for illegal goods, services and activities but it is also used to plan their illegal activities.

The Dark Web

Crowe, in conjunction with Cyfor and the University of Portsmouth, undertook research to find out more about how the Dark Web is used by criminals to support, plan, execute and monetise attacks on companies including financial institutions.

Findings included: -

- **What was for sale?** Fraud packs; template bank statements; utility bills; passports; UK bank account numbers / sort codes; template company cheques; and, advice on phishing.

- **How is it bad for business?** Fraud tools capable of being used to commit identity theft.

- **Sales of "Fraud Packs", with access to stolen personal data.** These contained bundles of information and guidance to assist with the commission of fraudulent attacks.

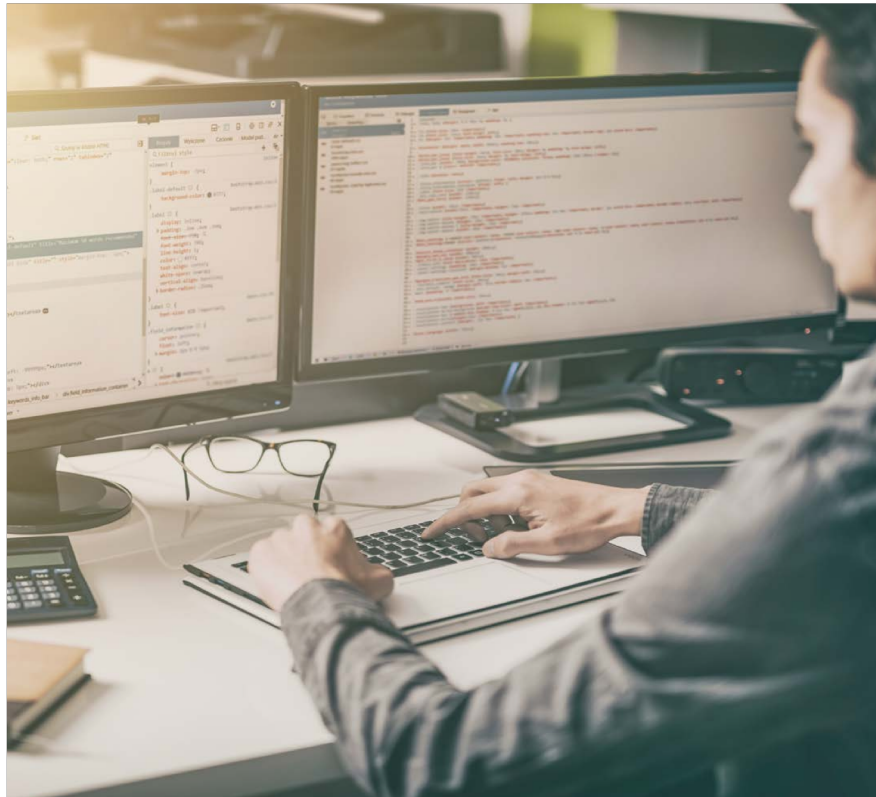
Cybercrime & Cybersecurity - Conclusion

Corporate Response

1. Risk Assessment
   - Identifying what to protect
   - Assessing the risk
   - Adhere to “International Best Practice”
   - Ongoing management involvement

2. Prevention
   - Privacy Policy & Security Manuals
   - Training
   - Cyber Insurance

3. Incident response
   - Emergency Response Team (Management, Legal, IT, HR and PR)
   - Securing evidence
   - Legal and IT advice
   - Police



Our Services

Crowe UAE – Cyber Developments

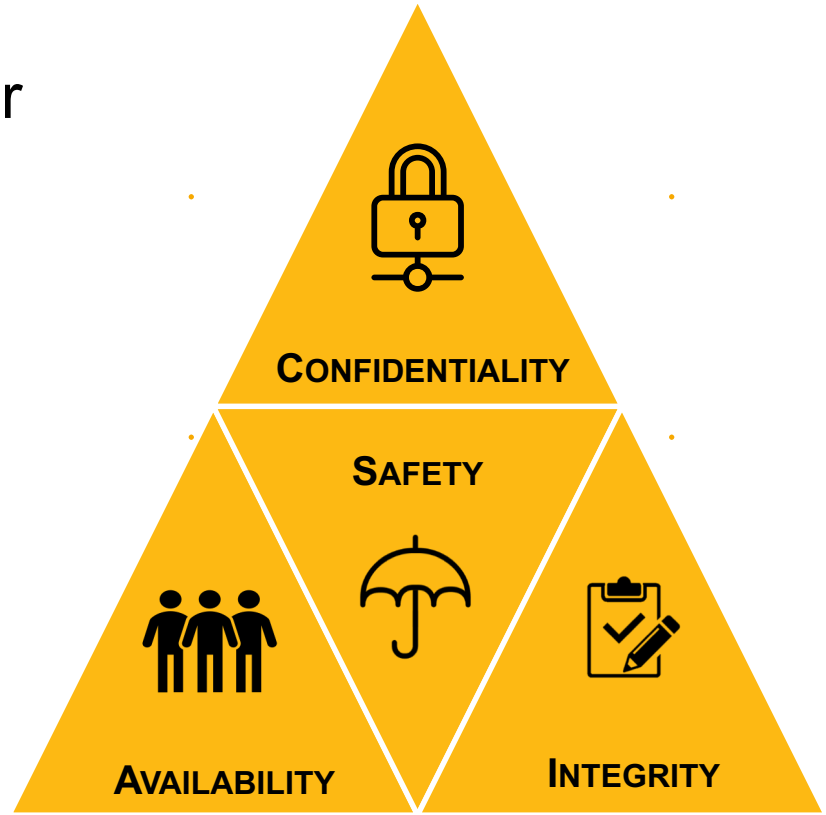
- Dubai to be resourced to become a Regional Hub

- Demand driven by market needs and increased regulatory focus
  - DFSA Thematic due in 2019
  - CBUAE instructions to regulated entities

- Launching full range of services with support from our global Centre of Excellence in Chicago . Services include: -
  - Strategic Evaluation
  - Technical Evaluation
  - Intrusion Testing
  - Incident Response
  - Cyber Defence
  - Dark Web Monitoring / Research

Why?...for Our Clients

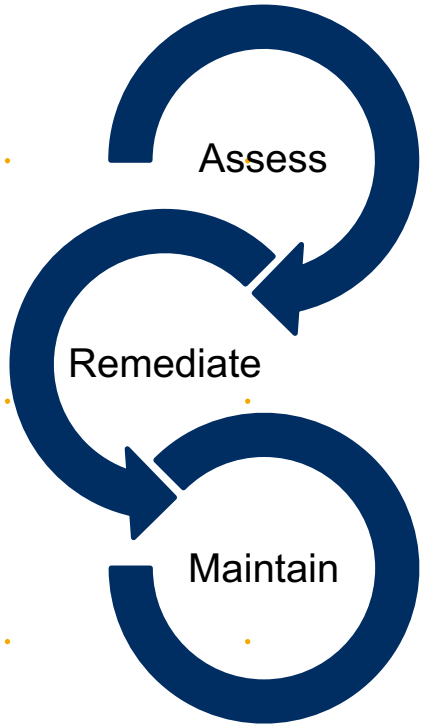
Crowe shares your priorities…**Clients.** We understand the importance of securing your sensitive information so you can focus on **what matters most**, serving your clients.



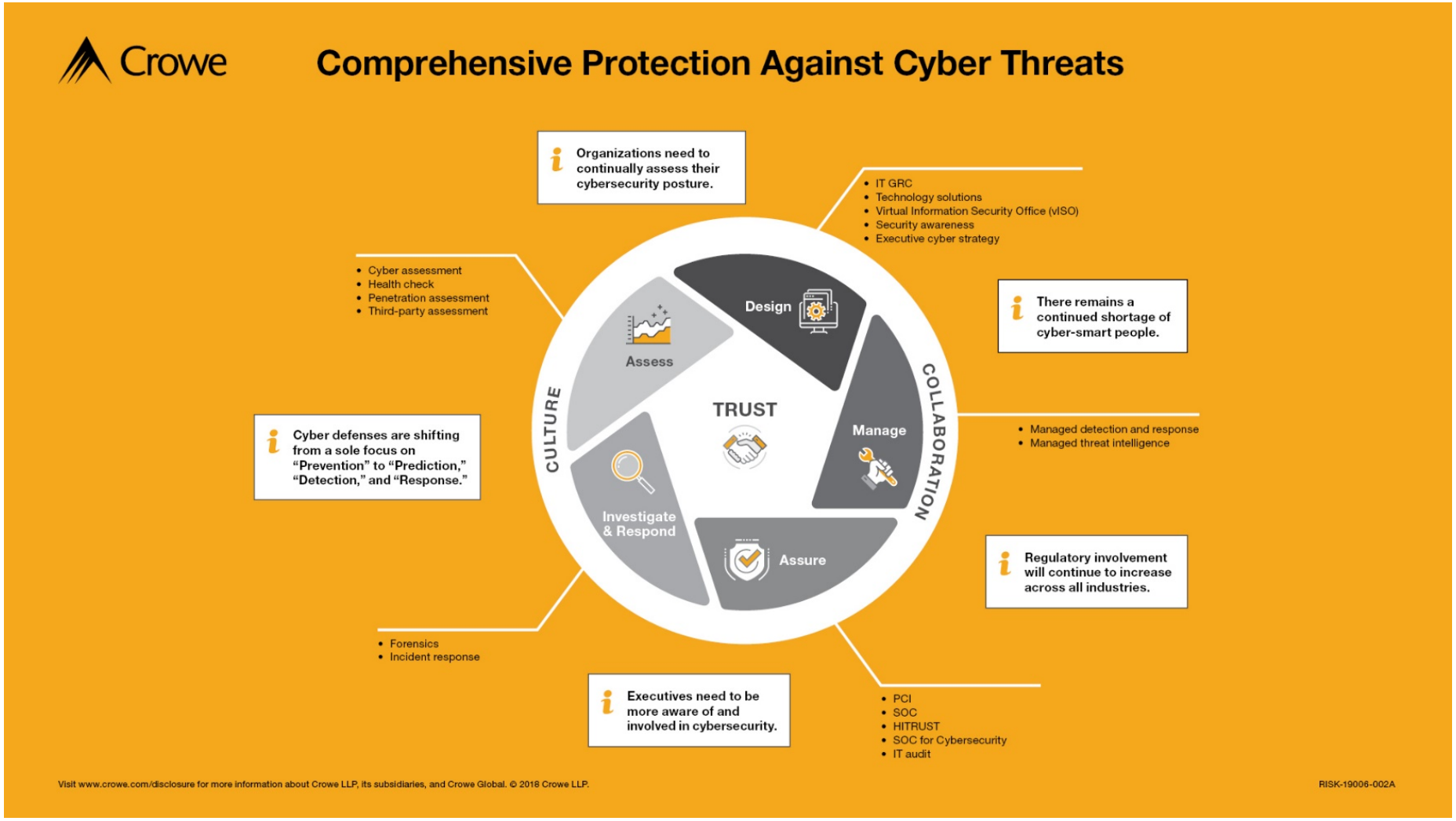
How? …the Power of Perspective

Our solutions takes a **holistic** approach to solving **your problems**. No solution is complete without considering the interplay between **people, process, and technology**

We meet you where you are. Whether your **risk** is **unknown**, seems **insurmountable**, or **beyond your reach** to manage, we are here to **help**.

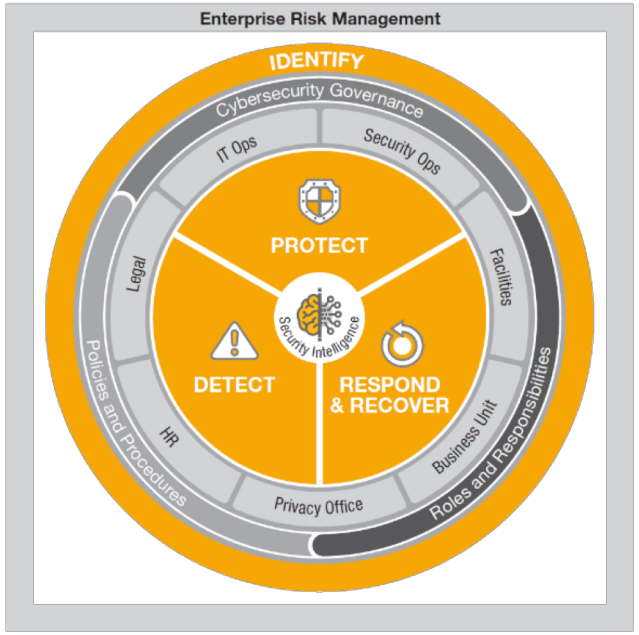


What?...Solutions that Fit the Risk Landscape



Crowe Cybersecurity Solutions Framework

At Crowe, we offer a full suite of technology risk and cybersecurity services designed to help organizations identify, assess, and mitigate data security risks. Facing increasing dependence on technology and an ever-growing array of internal and external risk factors, organizations of all types turn to Crowe to help them pursue a consistent, coordinated, and integrated approach to IT governance and cybersecurity risk management.



Crowe has worked with hundreds of companies across the globe to improve the quality of their Cybersecurity posture.

Each of our services is designed around a single cybersecurity framework that complements your organization's people, processes, and technologies.

Our solutions are designed to help your organization respond to the *major trends impacting your industry*.

Thank You

David Cafferty

+971 4 325 9900

+971 050 100 8558

david.cafferty@crowe.ae