Quest Masterclass

An Integrated Approach to Internal Auditing

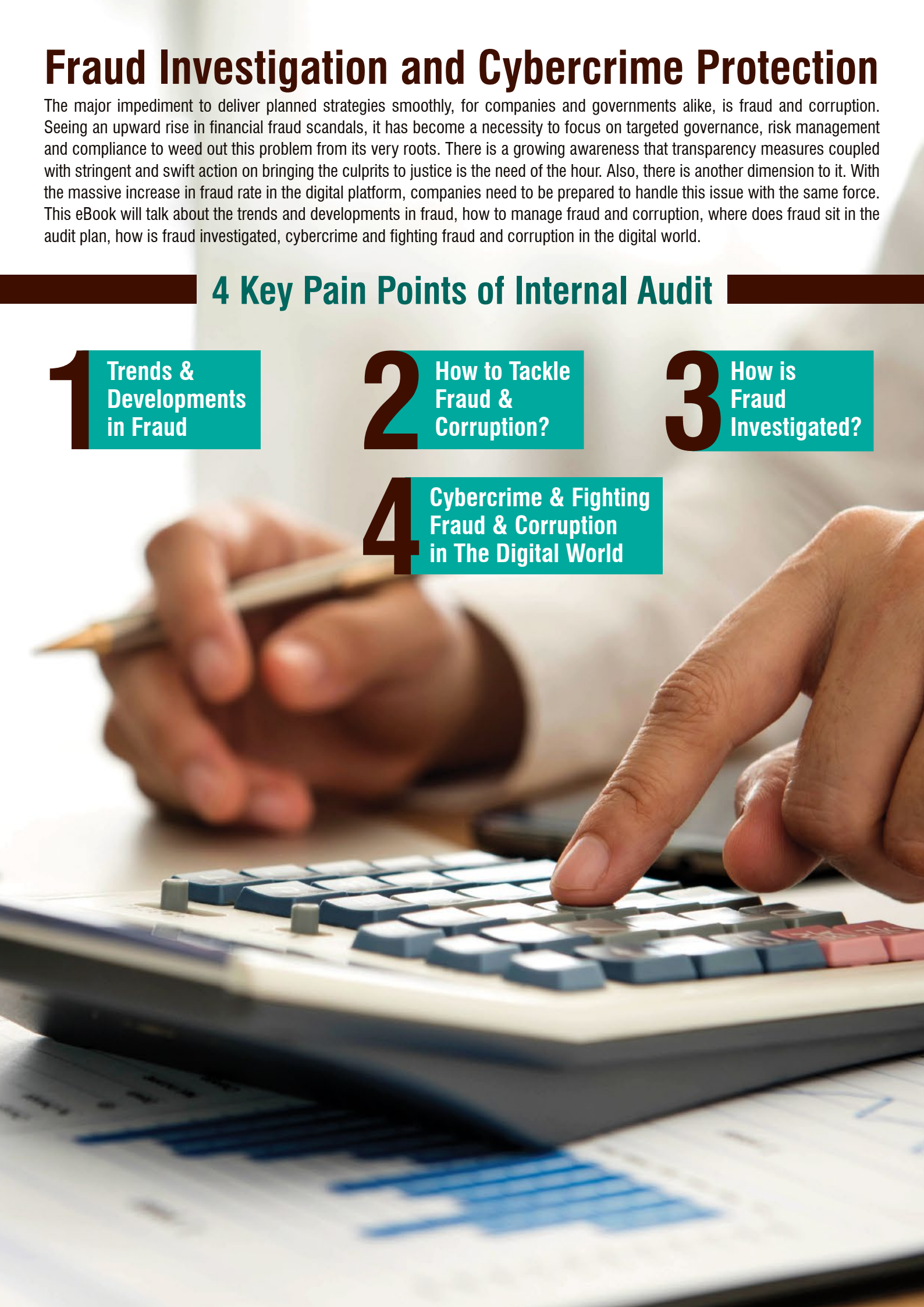
Dubai | June 2019

Fraud Investigation and Cybercrime Protection

The major impediment to deliver planned strategies smoothly, for companies and governments alike, is fraud and corruption. Seeing an upward rise in financial fraud scandals, it has become a necessity to focus on targeted governance, risk management and compliance to weed out this problem from its very roots. There is a growing awareness that transparency measures coupled with stringent and swift action on bringing the culprits to justice is the need of the hour. Also, there is another dimension to it. With the massive increase in fraud rate in the digital platform, companies need to be prepared to handle this issue with the same force. This eBook will talk about the trends and developments in fraud, how to manage fraud and corruption, where does fraud sit in the audit plan, how is fraud investigated, cybercrime and fighting fraud and corruption in the digital world.

4 Key Pain Points of Internal Audit

1. Trends & Developments in Fraud
2. How to Tackle Fraud & Corruption?
3. How is Fraud Investigated?
4. Cybercrime & Fighting Fraud & Corruption in The Digital World



1. Trends & Developments in Fraud

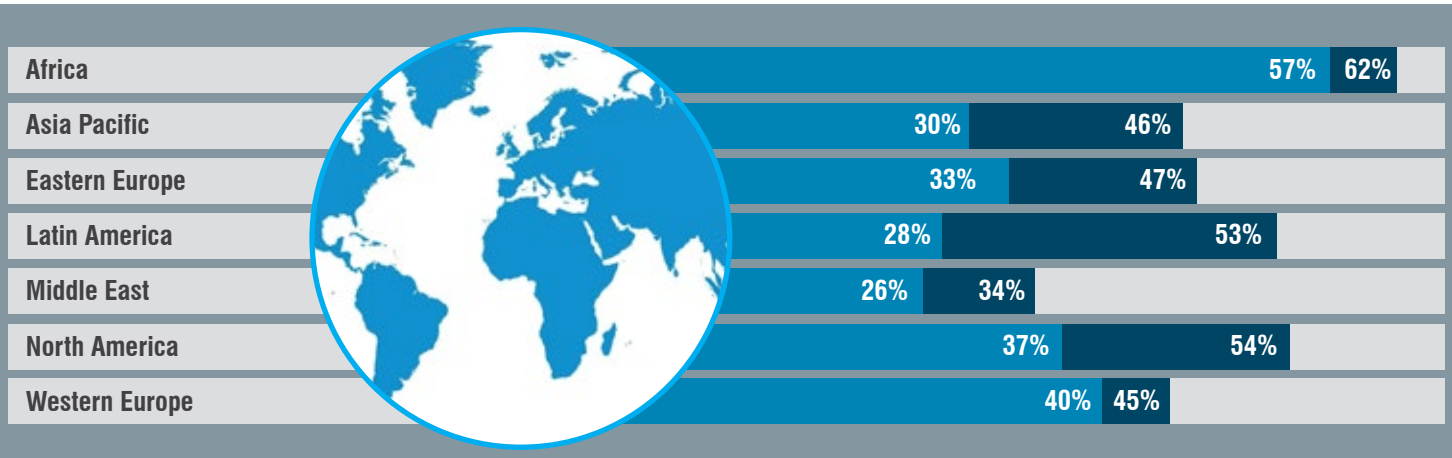
In the Middle East, economic fraud is on the rise. But on the good side, it's only 34% as compared to a global average of 49%. To combat this menace, 42% of the Middle East organizations are assigning large sums of money. And it is expected that this will increase to 49% in the next 2 years, which will be way ahead of the global average of 44%.

The Reported Economic Crime in The Region Has Increased from

26% to 34%

in The Past 2 Years

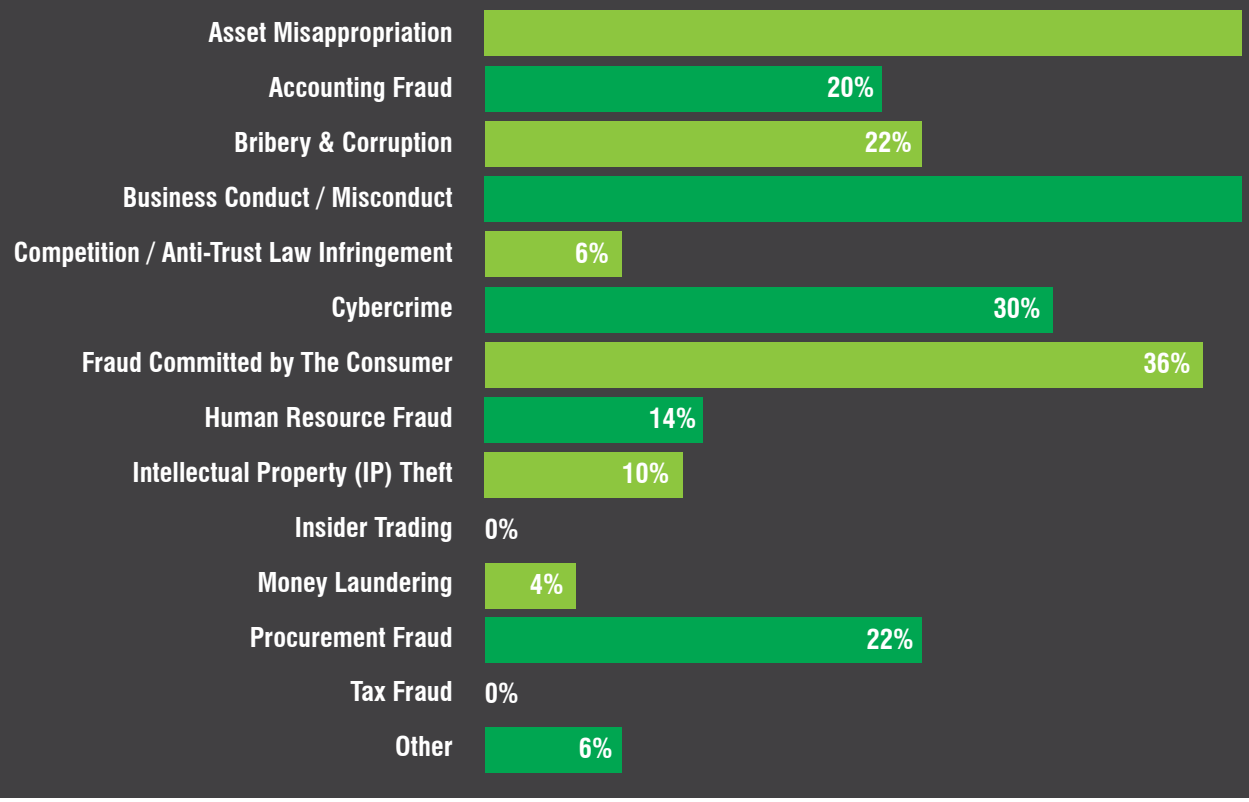
The Graph Gives A Visual Representation of The Increase in Economic Crimes Across The Globe



Source: PwC's Global Economic Crime and Fraud Survey 2018: Middle East Spotlight

The Graph Gives A Visual Representation of The Types of Economic Frauds Experienced, Arranged from The Highest to The Lowest

Types of Economic Crime / Fraud Experienced



2. Tackling Fraud & Corruption

Conducting a fraud risk is one of the most important functions of an internal auditor. It helps to identify how vulnerable is an organization to both, internal and external fraud. It also takes into account the organization's specific risk appetite. An internal auditor also needs to combat the expectation gap, needs to build a tandem between words and deeds, needs to define policies and procedures against bribery, corruption, and last but not the least, needs to put a strong whistleblowing policy in place. The info graphic below, depicts steps that can be used to effectively manage fraud:

- To Convey The Expectations of The Board of Directors, A Written Policy (or Policies) Should be in Place
- To Identify Specific Potential Schemes That The Company Needs to Mitigate, Fraud Risk Exposure Should be Assessed Periodically
- Detection & Prevention Techniques Should be Established Where Feasible, to Reduce The Possible Impact on The Organization
- A Coordinated Approach to Investigation & Corrective Action Should Be in Place, to Ensure That Corrective Action is Exercised at Once

After getting a brief understanding how fraud management is carried out, let's focus on a particular kind of fraud audit i.e., forensic audit investigation. The info graphic explains how such a fraud should be dealt with.

a. Investigation Planning

A — First & Foremost Recognize The Fraud That is Being Carried Out

B — Ascertain The Time Period for Which The Fraud Has Been Carried Out in The Organization

C — Look for The Factors by Which The Fraud Has Been Concealed So Far

D — The Next Step is to Track Down The Fraudsters Who Have Committed The Crime

E — Identify The Loss That The Organization Has Suffered Due to The Fraud

F — Collect The Relevant Evidence That is Admissible in The Court of Law

G — Educate The Employees & The Senior Management Team How to Prevent Such Frauds in The Future

b. Gathering Evidence

- Make Use of Substantive Techniques Such as Reviewing The Documents
- Make Use of Analytical Procedures That Help Compare Trends Over A Certain Period of Time
- The Auditor Should Make Use of Computer-Assisted Audit Techniques
- Comprehending Internal Control & Testing Them So as to Understand The Loopholes That Allowed The Perpetration of Fraud
- Interviewing The Suspect in Order to Gather Sufficient Evidence, So as to Make The Fraudster/s Confess His/her Mistake

c. Reporting & Indulging With The Court Proceedings

A

The Entire Matter Has to be Presented to The Client With Respect to The Fraud

B

The Report Will Help To File A Legal Case Against The Fraudster in The Court of Law

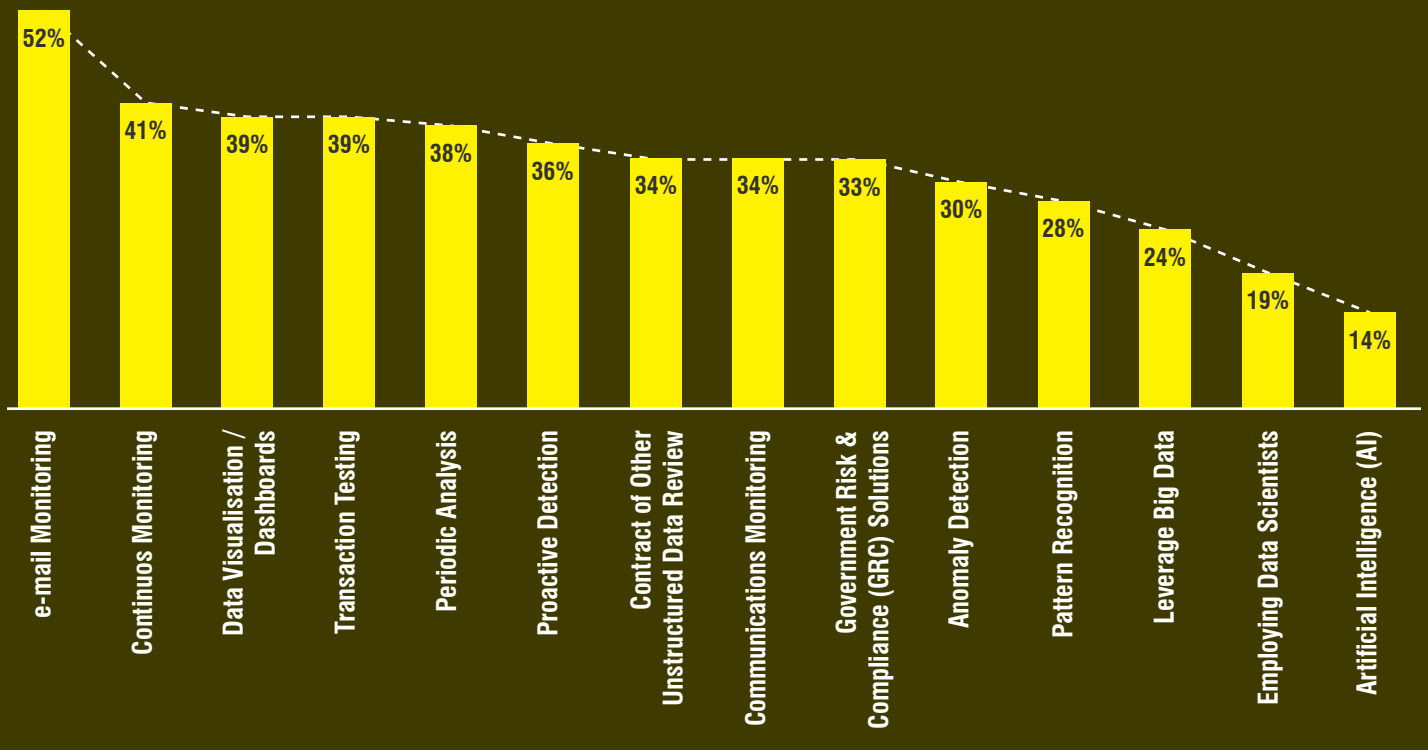
C

The Fraudster Needs to be Presented in The Court of Law as They Would be Required to Explain The Evidence Gathered Against Them

3. How is Fraud Investigated?

Companies are realising the importance of anti-fraud technologies in combating economic fraud and are increasing their usage at a rapid pace. **Put this quote on side of the previous two lines: According to PwC's Global Economic Crime and Fraud Survey 2018, 82% of respondents in the Middle East agree that continuous real-time monitoring assists their organisation in combating fraud.**

Measures Being Adopted to Combat Fraud Arranged from The Highest to The Lowest.



According to the above graph, we can see that more than half of the companies are considering email monitoring to combat the instances of fraud. The strategy ranges from monitoring email traffic continuously to carefully watching the exchange of electronic information over a selected period of time or a high risk area. Moreover, companies are readily focusing on email and chats for the purpose of sentiment analysis, to identify stress levels and patterns in the behaviour of employees.

52% of Organizations in The Middle-East Rely on Technology to Investigate Frauds with Respect to Cyber-Attacks and Vulnerabilities

4. Cybercrime & Fighting Fraud & Corruption in The Digital World

There were times when cyber-attacks coming to spotlight were once in a blue-moon incidence. But today hardly a day passes when large scale cyber-attacks are not the point of discussion across the globe. Recent cyber frauds have brought two things under scrutiny; that there are no cyber refuge shelters and that this is a worldwide phenomenon.

29% of Organisations Think Cybercrime is Likely to be The Most Disruptive Crime in The Next 2 Years

The most vulnerable industries by cyber-attacks are banks as they collect and process a vast amount of sensitive personal data. All forms of Personal Identifiable Information (PII) such as credit cards can lead to huge financial losses if in the hands of a wrongdoer. Also, cyber-attacks have the ability to interfere with the confidential information of a company. In short, cybercrime poses a major threat to tangible as well as intangible attributes of a business. They are discussed as follows:

1 Decrement in Customer Reputation and Stakeholder Confidence Due to Constant Data Breaches

2 Sharp Decline in Number of Customers

3 Steep Shrinkage of Revenue

4 Loss of Owned Data and IP

5 Major Interruption in The Proper Functioning of Business

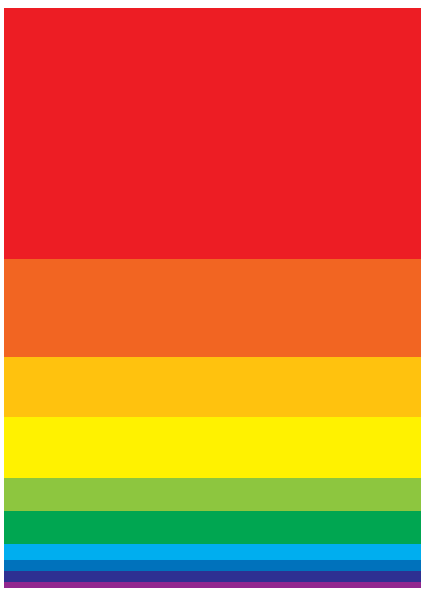
6 Legal Costs Arising Out of Penalties and Litigations

7 Steep Decrease in The Share Price Because of The Above Arguments

77% of Organizations Have A Cyber-Incident Response Plan Up From 33% In 2016

Moreover, law enforcement agencies are too lazy when it comes to solving cases relating to cybercrimes. And this is evident by the following three reasons:

1. As compared to lightning speed of technological innovation, legal procedures are awfully slow.
2. Cyber-attacks easily occur across borders, which creates additional problems to cope up with international laws.
3. By the time courts look for legal remedies, the damage has already been done.



Malware / PoS Malware	43.3%
Unknown	17.0%
Targeted Attack	10.4%
Vulnerability	10.4%
Account Hijacking	5.7%
DDoS	5.7%
Malicious Script Injection	2.8%
Credential Stuffing	1.9%
Misconfiguration	1.9%
Defacement	0.9%

10 Steps to Cybersecurity According to National Cyber Security Center

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User Education and Awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware Prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable Media Controls

Produce a policy to contol all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure Configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing User Privilages

Establish effective management processes and limit the number of privileged accounts. Limit user privilages aand monitor user activity. Contril access to activity and audit logs.

Incident Management

Establish and incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

Today, there exist myriad programmes on Internal Audit but unfortunately, most of them are devoid of tools, which can train auditors on how to deliver competitive advantage to a company, and how they can develop an Audit strategy that is perfectly aligned to the business strategy. In our 3 day workshop, Chris Hollands, will teach you how to sail your way through the nitty-gritties of Internal Audit, by covering topical areas like Money laundering, Terrorist Financing, fraud and forensic auditing as well as other areas that pose a challenge to internal auditors. The course will also spend time on developing 'soft skills' that all business professionals, but particularly Internal auditors, need to improve upon, covering all effective communication in all its forms, both at individual and at departmental level. We urge you not to miss this opportunity, and take-home expert Internal Auditing skills and increase the productivity to higher level.

Quest ontheFRONTIER

People- Knowledge- Success

Consulting/
Interim Management

Executive Search

Master Class &
Conference

Incorporated in 2002 and head quartered in Singapore, **Quest ontheFRONTIER** is an established international consulting, executive search and training company operating in Asia, the Middle East and Africa with 7 offices including China, India, Vietnam and Indonesia. We provide implementation consulting wherein our consultants with deep industry knowledge help organizations develop and execute business initiatives. The same philosophy guides our training services including Quest Master Class; our Master trainers are seasoned industry executives with leading global companies who share their insights and facilitate interactive learning among the participants. Quest conferences provides a platform for industry leaders to exchange ideas, interact and network.
We help individuals and organizations succeed through knowledge and insights.

Quest Masterclass

Quest Conferences

Quest Learning & Development

Quest Consulting

www.questonthefrontier.com

Singapore l Hong kong l China l Vietnam l India l Indonesia l Dubai UAE l Myanmar

for More Details Contact Upendra@questmasterclass.com