Crowe

Internal Audit Transformation: Surviving Key in Disruptive Era

Audit | Tax | Advisory | Capital Market

Smart decisions. Lasting value

Overview

The era of uncertainty approaches sooner as disruptive innovation creates a new market replacing currently established market-leading firms and products. Several examples of innovation which change our business and society are as follows: telephony replaced telegraphy, smartphones replaced personal computers & laptops, and word processing app replaced typewriter. New innovation in technology enables the creation of new business model or the modification of current business model.

Based on our overview above, below is a real story on how a new start-up company faces unprecedented risks due to technological innovation.

Fake bookings

Popular Indonesian motorcycle ride-hailing app gained its momentum in recent year. The growth couldn't be stopped since its brings more income and efficiency for its drivers, and better safety solution and transparent fares for its passengers compared to the independent & informal motorcycle taxi drivers. The innovation brings company-wide opportunities, not only in traditional business model such as transportation, logistics, and food delivery sector, but also in mobile payments, and many other contemporary lifestyle on-demand services.

The fast growing business also brings unprecedented challenges where the company detected more than 7.000 drivers cheating its own booking system. This can be done by creating fake bookings, in which the driver snatches up the booking and collects the payment, but never actually performs the ride.

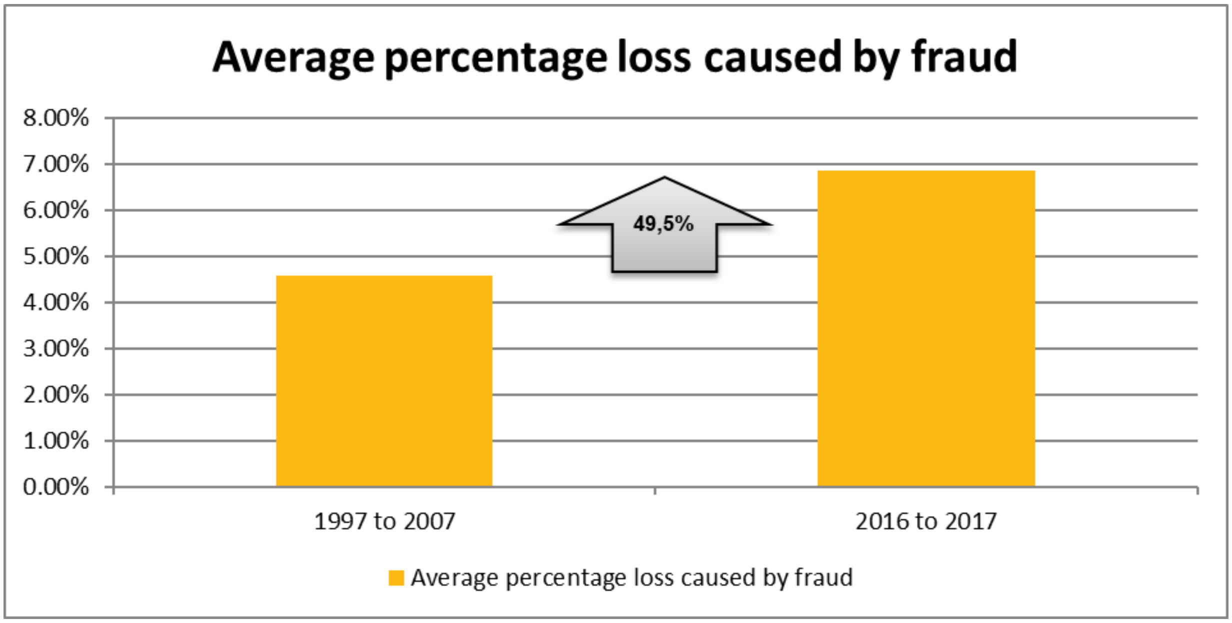
The cheating escalated and became uncontrollable when external actors got involved. The external fraudsters offer fraudulent applications that can hijack the booking application. Moreover the fraudsters offer not only the applications but also accommodating devices at affordable prices.

The Company founder, in a brief statement, argued that the company has collected sufficient evidences against these drivers, and needed to take a strong stand to discourage future fraud attempts. However, there is a possibility that some drivers did not cheat, they were snatched up by corporate fraud detection algorithms by mistake instead.
(source: techinasia)

Key Challenges

Industries, ranging from retail to transportation are increasingly being disrupted by new technology and ideas. This is creating a shift as innovative firms are swallowing market share from incumbents. The combination of tech-savvy applications, new ideas, customer behavior changes, and government regulations results in fertile conditions for disruptions to thrive. The explosion of new technology and new innovation that accompany it brings unpredictable new risks and opportunities.

Fraud is a pernicious problem and its economic impacts are clear. Online transportation as a new business models also got affected by this deliberate deception. Based on 2018 Financial Cost of Fraud Report released by Crowe UK and Centre for Counter Fraud Studies (CCFS) at the Institute of Criminal Justice Studies, University of Portsmouth, the global average loss rate for the entire period of the research (5.95%), when taken as a proportion to the global Gross Domestic Product (GDP) for 2017 (USD 75.278 trillion or £54.381 trillion).



Moreover, from comparative chart below, Crowe UK and CCFS noted that since the start of the global recession in 2008, there has been an increase in average losses from 4.57% to 6.84% for the period 2016 to 2017 – an increase of 49.5%.

According to the research, the growth of fraud is allegedly caused by social and technological factors besides the economic cycle factor. Some of the factors might include:

- Greater individualization (less adherence to collective moral and ethical 'norms').
- Greater complexity of processes and systems (it is becoming easier to disguise fraud amidst this complexity).
- More transactions being undertaken by computer and fewer face-to-face transactions (fraudsters feeling more distant from the victims and thus less concerned about any response).
- The increasing pace of changes in business (with controls struggling to keep up).

Hence, internal audit especially those in the technology-reliant industry should be aware and anticipated such phenomena. The utilization of leading-edge technology could generate a double-edged result where it could bring great opportunities and also potential risks. From the story we presented above, the fraud attempted did not only committed by internal parties but also external parties whom the company never, ever or had been in business relationships such as apps vendors, shared service providers, ex apps vendor, previously shared service providers or external hackers.

Internal Audit Transformation in Disruptive Era

Rapidly advancing technology, political and economic shifts, and ever-changing regulations make the risk landscape highly complex. Moreover, Internal Audit (IA) function is expected to give an insightful guidance for organizational leaders to tackle emerging risks in competitive era. In regards to the case we mentioned at overview section, we recommend several actions which should be performed by internal audit as follows:

- **Managing expanding risk universe**
  Internal audit needs to wisely dedicate its limited resources to address an expanding risk universe. Nowadays, the internal audit plan is shifting its focus from financial and compliance risks to a broader view that includes operational and strategic risks.

- **Emphasis on building effective internal control**
  Internal audit should continue to focus on building effective internal control regardless of the arrival time of disruption. By continuing to focus on risk management, control, and governance, internal auditors can help ensuring that processes are designed and operating effectively. Finally, by proactively helping the organization to anticipate emerging risks and technological changes, internal audit can be positioned as an authority and help preparing the organization to respond to disruptive events.

- **Focusing on third-party service providers**
  A survey performed by Crowe US found that 65 percent of respondents across industries make significant or extensive use of third-party vendors and ninety-one percent indicated that technology vendors are significant to their business model.

  As use of these vendors has ramped up, so does the incidence of breaches originating from third parties rather than the breached entity itself. Of course, the breached entities suffered reputational damages and/or financial losses despite their lack of culpability.

  From the survey result, it can inferred that many of the breaches have targeted multiple points of weakness, including:
  - Vendor-owned or managed systems
  - Vendor remote access to the company system
  - Information provided to third parties
  - Information entered into third-party provider websites

- **Maintaining documented description of cryptographic architecture**
  Company must understand all algorithms, protocols, and cryptographic keys protecting its system architecture. Internal audit should reassure management keep inventory of all key management devices, including host security modules and secure cryptographic devices.

- **Detecting and reporting failures of critical security control systems**
  Management must have formalized procedures for detection and documentation of the failures and documentation of the restoration of failed security functions. The compulsory step is needed to reduce the period of time between discovering and reporting a breach.

- **Performing penetration testing regularly**
  IA should ensure that management performs the penetration testing regularly. Additional testing is still required after any changes in system is performed.

- **Performing review over security policies and operational procedures**
  Internal Audit needs to validate whether management personnel are following IT security policies and operational procedures. IA should get reasonable assurance that existing IT policies and procedures are being followed with daily logs, firewall rules, configuration standards, security alert response, and change management.

- **Boosting efficiency using data analytics**
  In the past decades, the usage of data analytics software brought tangible contribution in reducing auditing and monitoring costs. With data analytics ability, internal audit team could review the whole population (not only sample). Moreover, advanced data analytics usage facilitates early prevention and detection of fraud, abuse, errors and regulatory non-compliance.

  Finally, by designing and adopting cutting-edge data analytics capability, Internal Audit can boost its productivity and efficiency, thus it will have more resources to allocate in operational and strategic areas.

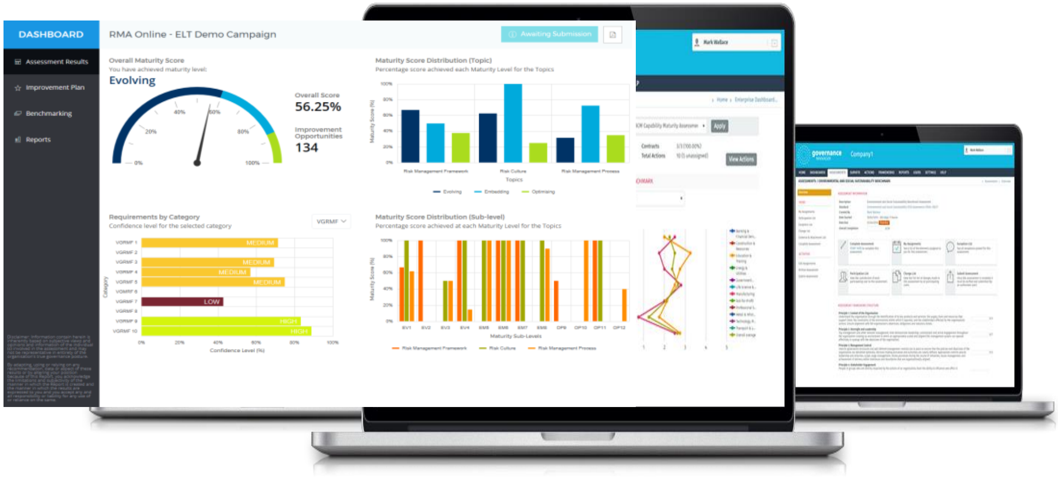
- **Looking ahead**
  Partly in response to technological innovations, along with changes in corporate structure and competitive business factors, internal audit needs access to a broad range of skills to fulfill its mission. Internal audit transformation is vital as the function serves the business with high-level business insight. Organizations gain benefits when internal audit is capable to handle not only regulatory and compliance matters, but also to help manage risks that are operational and strategic in nature.

Governance Manager

IA Organizations of all sizes need fine tuning to improve their performance and to become more resilient with the development of new technology and new business ideas. Having a formal system (beyond excel spreadsheets) for measuring and improving internal audit capability maturity is increasingly demanded by boards and management.

Having a formal system to measure organizational maturity is essential. Governance Manager, a cloud-based platform puts the power for measuring maturity in your hands and boosts performance with business insights. Developed by leading advisory firm Blue Zoo, the platform stipulates capability in performing benchmarking, strategic improvement and quality insights.

The platform enables executive monitoring and capability insights at a strategic level. It is done by automating capability maturity self-assessments, comparative analysis of federated environments, and by focusing resources on improvements. Hence you can easily deploy the best practice references that are important for your business to mature and succeed.



How Crowe Helps

Crowe internal audit professionals have years of experience gained through internal audit services for diverse and complex companies across a range of industries. This extensive experience provides us with in-depth knowledge of the needs and problems facing our clients.

- **Experienced Team Leadership.** Crowe provides direct, executive-level involvement in every engagement.
- **Commitment to Stakeholders.** Crowe develops effective communication with top level management client to deliver the right message regarding the project.
- **Technological Expertise.** We draw upon specialists in many disciplines and we can include a technology specialist in your team.
- **Applicable Methodology.** Crowe leverages a methodology that has direct impact to the client.
- **Testament of Quality.** Crowe is nationally recognized for providing a wide range of risk services.
  - Crowe is recognized by the IIA as an IIA Principal Partner.
  - Ranked the eighth largest accounting network in the world and sixth largest accounting network in Asia Pacific, Crowe has over 220 independent accounting and advisory firms in more than 130 countries.
  - Forbes best management consulting firms for 2018.
  - Fortune 100 Best Companies to Work for 2018.

Connect with us

Lugbi Wyndiartanto
Risk Advisory
Crowe Indonesia

Office +62 21 2553 5699
lugbi.wyndiartanto@crowe.id

Jurita Suharto
Risk Advisory
Crowe Indonesia

Office +62 21 2553 5699
jurita.suharto@crowe.id