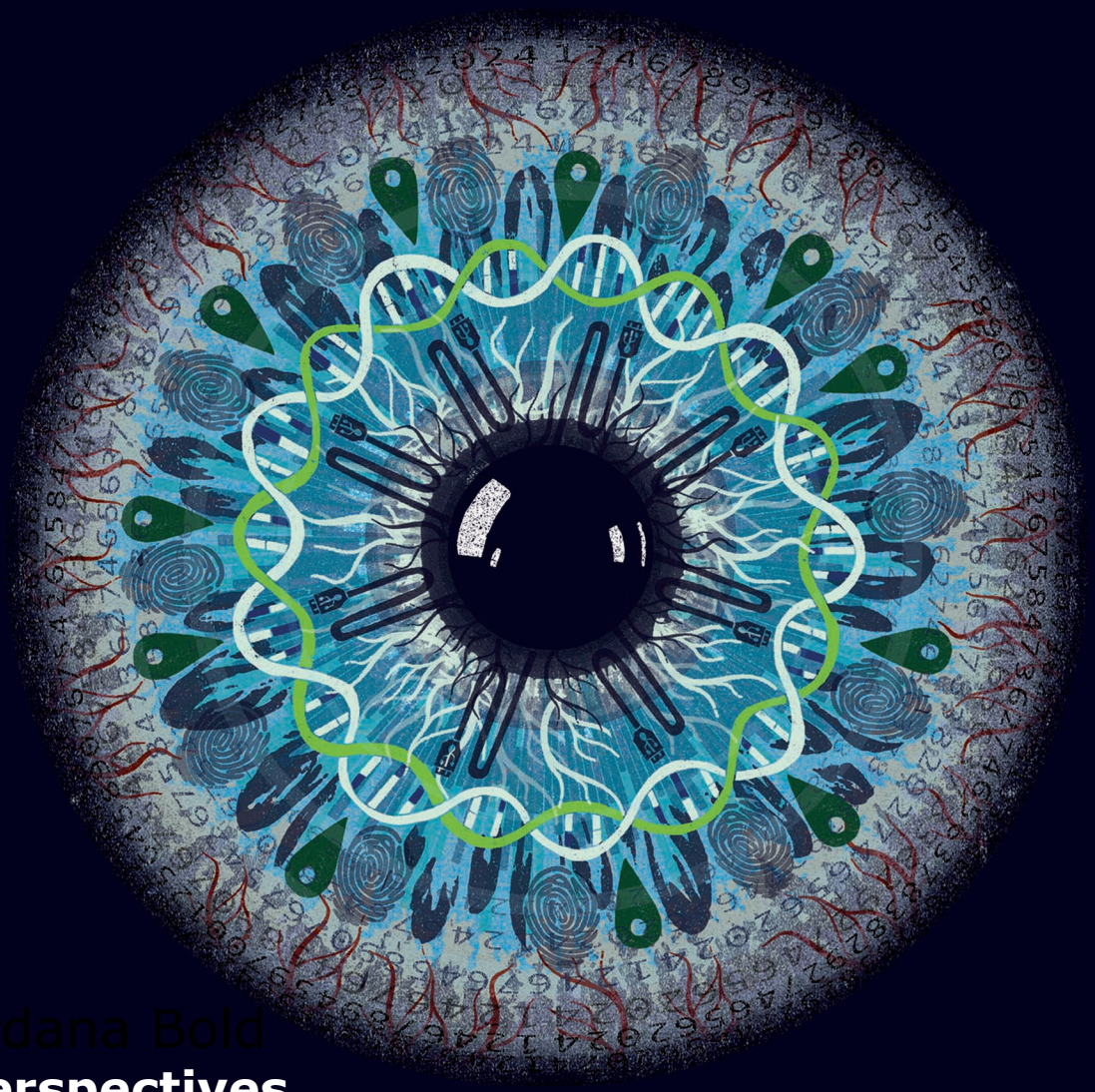
Deloitte.



Headline Verdana Bold

Malaysian Perspectives

On Cyber Readiness

Megat Mohammad Faisal

10 October 2017

Setting the scene on Cyber Readiness

The Hiscox Cyber Readiness Report 2017 stated that ….

72%

US firms are the most likely to have experienced an attack with 72% of larger businesses reporting a cyber incident in the past year and nearly half (47%) of all US firms experiencing two or more.

55%

Take-up of cyber insurance remains heavily skewed to the US with 55% saying they have taken out cyber insurance compared to 36% in the UK and 30% in Germany.

49%

Nearly half of the 'expert' group in our cyber readiness model is made up of US companies.

43%

German businesses are the least likely of the three countries to believe that their government's policies are supportive, with only 43% agreeing that their government is doing enough to protect them.

39%

Germany lags behind in terms of cyber readiness. German firms make up the biggest group of cyber novices (39% of the total) while UK and US firms account for 36% and 26% of the total respectively.

33%

Over a third of German firms are not interested in cyber insurance. That is more than twice as high (15%) as the US.

45%

UK firms are the least likely of the three countries to have experienced a cyber-attack in the past 12 months, with 45% saying they have had no incidents in that time.

45%

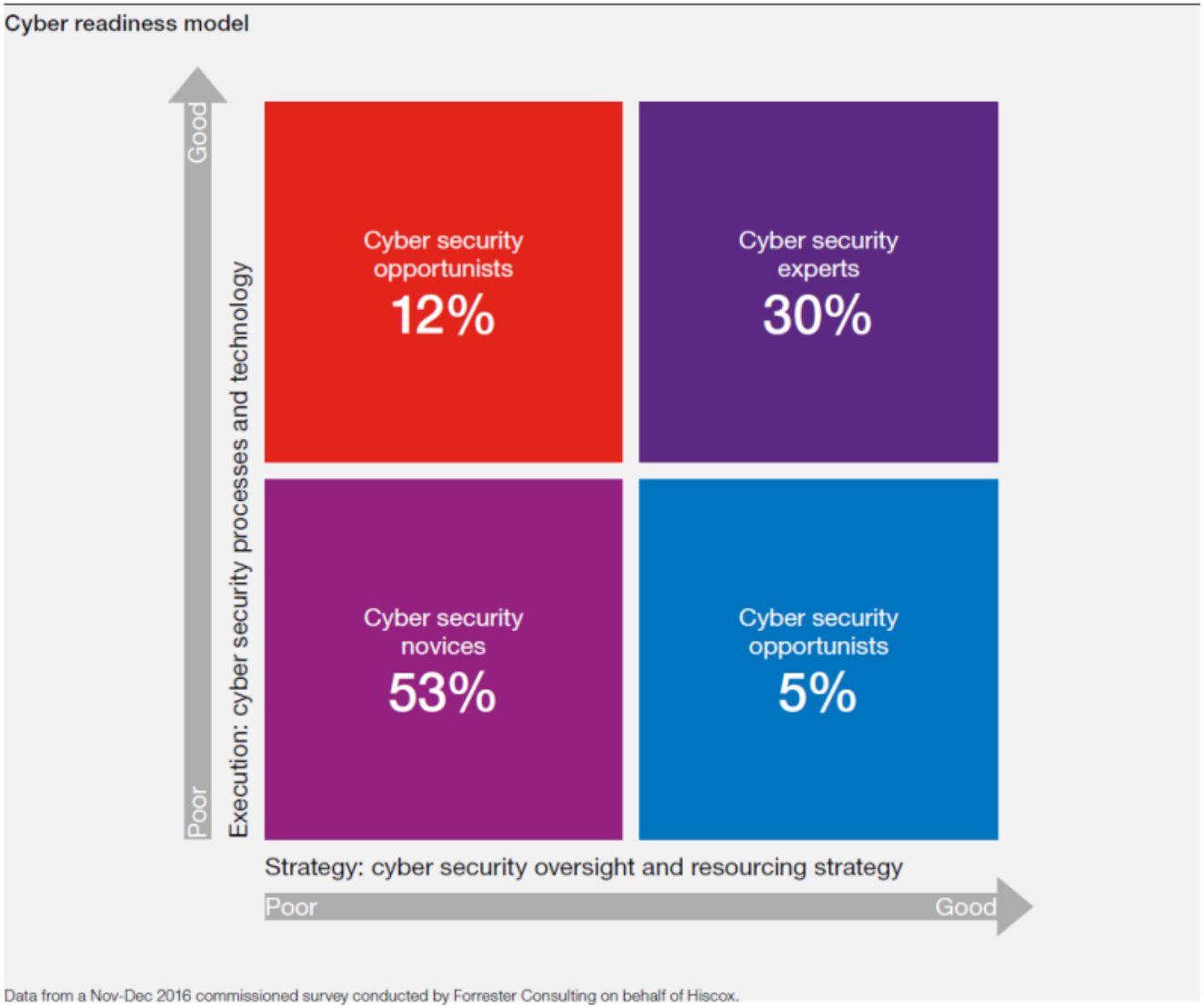
UK firms are the most likely to think that a cyber insurance policy is not relevant for them with 45% having no plans to take out insurance.

35%

Over a third of UK businesses say that they have changed nothing following a security incident in the past 12 months.

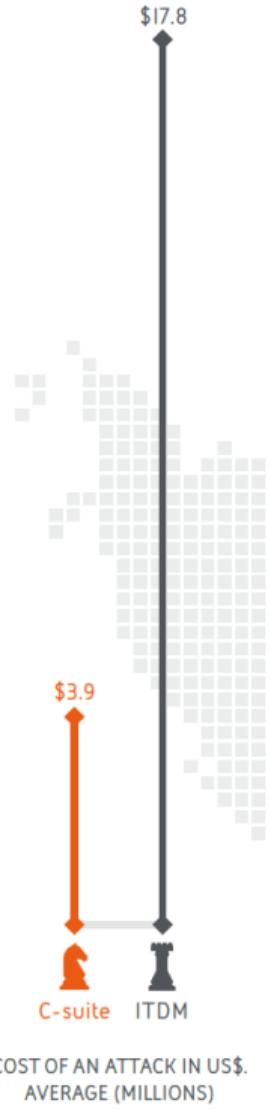
Setting the scene on Cyber Readiness

The Hiscox Cyber Readiness Report 2017 stated that ….



Setting the scene on Cyber Readiness

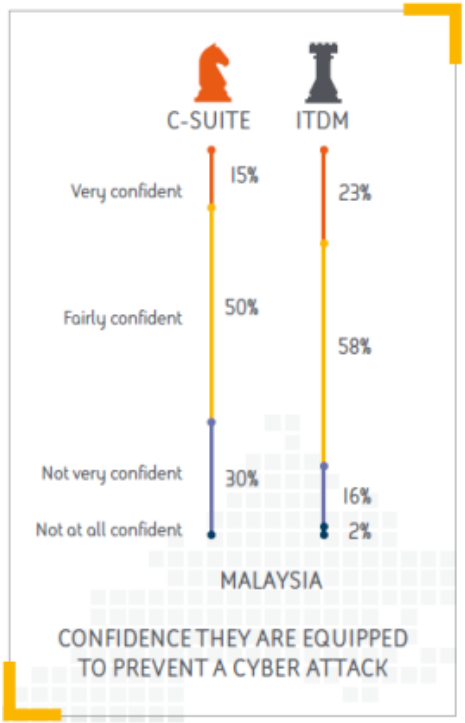
BAE's 2017 Cyber Defence Monitor Report on Malaysia stated…

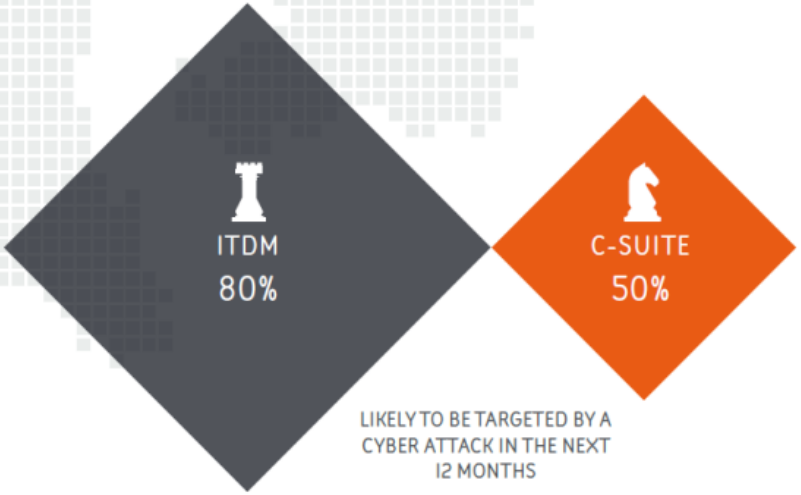


COST OF AN ATTACK IN US$. AVERAGE (MILLIONS)

90% of C-suite believe the number of attacks will increase next year

Only 2% of **ITDMs** belive they have the right skills in house





LIKELY TO BE TARGETED BY A CYBER ATTACK IN THE NEXT 12 MONTHS

Readiness, response, and recovery

Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data, and other cyber incidents have become commonplace. It's enough to leave one thinking—correctly— that no organization can achieve totally assured cybersecurity.

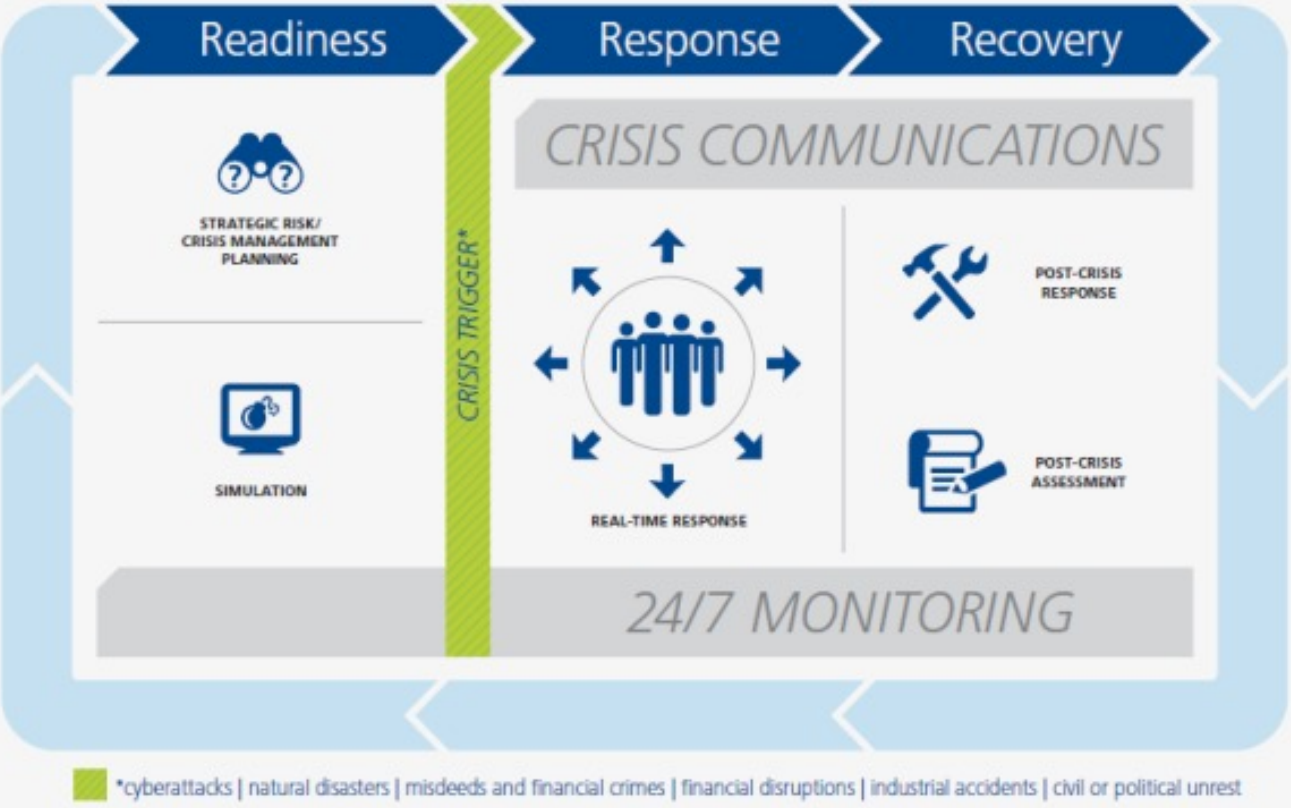
The need for crisis planning

CBS.com notes that 1.5 million cyberattacks occur every year, which translates to over 4,000 attacks every day, 170 every hour, or nearly three every minute.[1] While few attacks succeed, the high probability of cyber incidents dictates that every organization needs to be prepared to respond effectively.

[1] CBS News. *These cybercrime statistics will make you think twice about your password: Where's the CSI cyber team when you need them?*

Exhibit 1

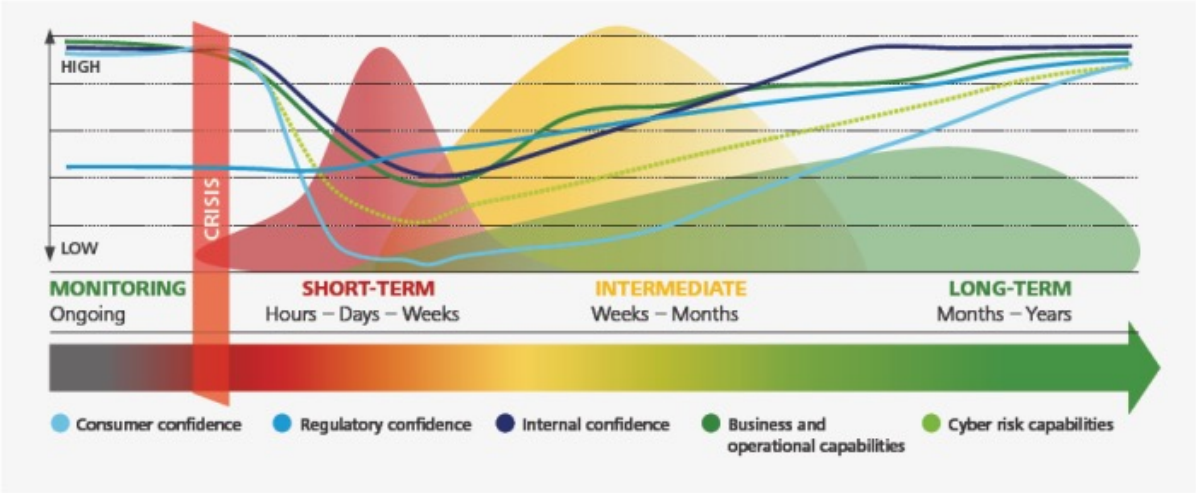
Deloitte's crisis management lifecycle



The cyber incident response lifecycle

While the precise nature, location, and impact of incidents cannot be predicted, the incident response lifecycle follows a predictable path (see *Exhibit 2*).

Exhibit 2
Cyber incident response lifecycle



Getting coordinated

Cyber incident response programs require coordination in six key areas: governance, strategy, technology, business operations, risk and compliance, and remediation.

1 Governance

Governance frames the way you organize and manage your response team. It ensures program coordination across functional areas, documentation of all policies, procedures, and incidents, and clear communication roles, responsibilities, and protocols. Governance aligns response strategy with goals and provides mechanisms for cross-functional communication.

Exhibit 3

Cross-functional capabilities required for effective response

2 Strategy

Response strategy defines how you lead, prioritize, and communicate during incident response and crisis management. Organizations should align response strategy with the organization's responsibilities and values. A sound strategy frames a cost- effective, well-resourced, organization-wide approach to addressing cyber incidents. This minimizes "tunnel vision" in response planning and reduces adverse impact to operations and revenue.

Key aspects of response strategy include:

- Defining escalation and prioritization processes to manage and coordinate IT, operational, and business recovery
- Engaging the organization's government affairs team or other government liaison function to inform and work with regulatory agencies and any appropriate officials—an essential step in any regulated industry
- Aligning response efforts with security management and IT engineering initiatives

Cyber Strategy Framework (CSF)

Managing cyber risk to grow and protect business value

The Deloitte CSF is a business-driven, threat-based approach to conducting cyber assessments based on an organization's specific business, threats and capabilities. CSF incorporates a proven methodology to assess an organization's cyber resilience; content packs which enable us to conduct assessments against specific standards; and an intuitive online platform incorporating a range of dashboards that can be customized for an executive, managerial and operational audience.

Three fundamental drivers that drive growth and create cyber risks:

- **Innovation**
- **Information sharing**
- **Trusting people**

CEO:
"I read about phishing in the news. Are we exposed?"

CIO:
"Where and how much do I need to invest to optimize my cyber capabilities?"

Board:
"What is our level of resilience against these cyber attacks?"

Organizations need a holistic, business-driven and threat-based approach to manage cyber risks. While securing assets is important, being vigilant and resilient in the face of cyber attacks is imperative

Business risks

What is my business strategy?

What is my risk appetite?

What are my crown jewels?

Threat landscape

What are they interested in?

What tactics might they use?

Who are my adversaries?

Cyber capabilities

Governance
Identify top risks, align investments, develop an executive-led cyber risk program

Secure
Take a measured, risk-prioritized approach to defend against known and emerging threats

Vigilant
Develop situational awareness and threat intelligence to identify harmful behavior

Resilient
Have the ability to recover from and minimize the impact of cyber incidents

A strong cyber risk program helps drive growth, protects value and helps executives to be on top of cyber threats

1. Understand the business context and objectives
2. Understand my threat landscape
3. Understand current maturity level of cyber capabilities
4. Focus on the right priorities
5. Define target maturity level of cyber capabilities and recommendations
6. Develop cyber strategy roadmap
7. Enhance value from cyber security investments
8. Communicate with internal and external stakeholders

3 Technology

The IT and cybersecurity teams develop and implement mechanisms for detecting, monitoring, responding to, and recovering from a cyber incident or crisis. IT engineers create the needed architecture, and IT works to maintain systems that are resistant to attacks.

Key questions

- Which incident and crisis mitigation techniques are we employing?
- What technical capabilities do we have, and what are we missing?
- Do we have access to forensic resources?
- How are we gathering and using threat intelligence?

4 Business operations

After an incident, critical business operations must resume as soon as possible to minimize disruptions that generate financial, reputational, regulatory, and stakeholder impacts.

Keys to minimizing business disruption include:

- Implementing out-of-band processes to replace those that are broken or that present too many constraints during incident response or to remediation
- Planning for surge support and allocating resources accordingly
- Understanding existing business limitations, such as the risks associated with using standard payments systems or certain applications

5 Risk and compliance

Risk and compliance functions should assess and manage the regulatory compliance elements of incident and crisis response, including interfacing with legal counsel, regulators, and law enforcement. The keys are to be able to comply with requirements and to demonstrate compliance. For example, after an incident, investigative processes and responses must be documented to demonstrate the adequacy of both.

Key questions

- What are the breach notification requirements?
- What are the regulatory and third-party obligations?
- When and how do we inform law enforcement?
- How could this particular incident— or a pattern of incidents—impact the organization's compliance posture?

6 Remediation

Remediation begins after critical business operations resume, with short- and long-term efforts to close gaps. The organization must verify that attack vectors are eradicated and take steps to prevent similar attacks in the future. Remediation must eliminate or minimize root causes of incidents and return businesses, functions, IT, and stakeholders to a secure operating environment.

Key questions

- Have the IT and business-process root causes been identified?
- Has a remediation plan been developed?
- Have the root causes been eliminated or minimized?
- What are the lessons learned and how can we apply them?

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organisation of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 135,000 people worldwide, Deloitte delivers services in four professional areas—audit, tax, consulting and financial advisory services—and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names.