



Kuwait 5th ERM Conference

The Board's Eye View of Cyber Risk

Presented By:

Fadi Mutlak

Partner – Risk Advisory

Deloitte

fmutlak@deloitte.com

Jan 2019



The Digital Revolution



Pervasive digitization, open and interconnected technology environments, and sophisticated attackers, among other drivers, mean that the risk from major cyber events could materially slow the pace of technological innovation over the coming decade. Addressing the problem will require collaboration across all participants in the “cyber resilience ecosystem”

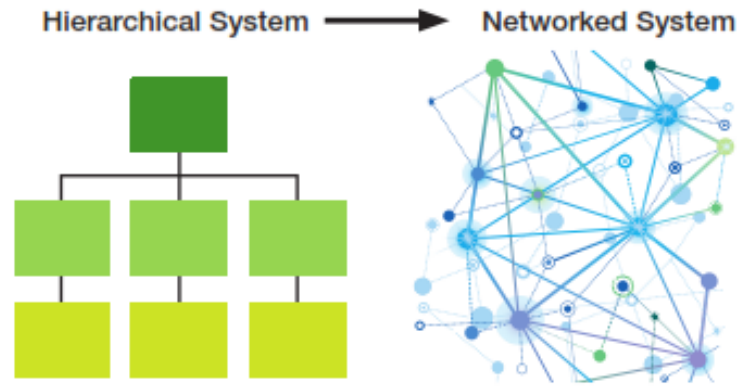
The Digital Revolution

World Economic Forum – Hyperconnectivity & Hyperdependence

Hyperdependence

The concept of de-perimeterization has emerged in the last decade **as the borders between the internal and external networks are becoming less clear.** Employees increasingly use their own devices for work purposes; partners, contractors and customers share access to networks and cloud-based services continue to enjoy rapid growth.

Hyperconnectivity



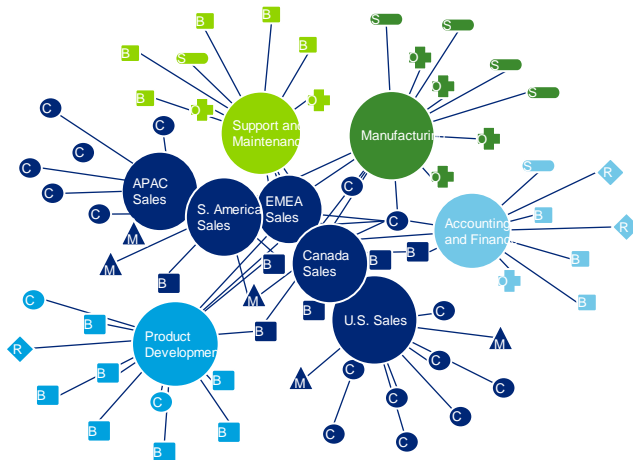
Connectivity of Things:

The risk of this “**connectivity of things**” has been described by Rod Beckstrom in terms of “laws”:

Law 1: Everything connected to the Internet can be hacked

Law 2: Everything is being connected to the Internet

Law 3: Everything else follows from the first two laws



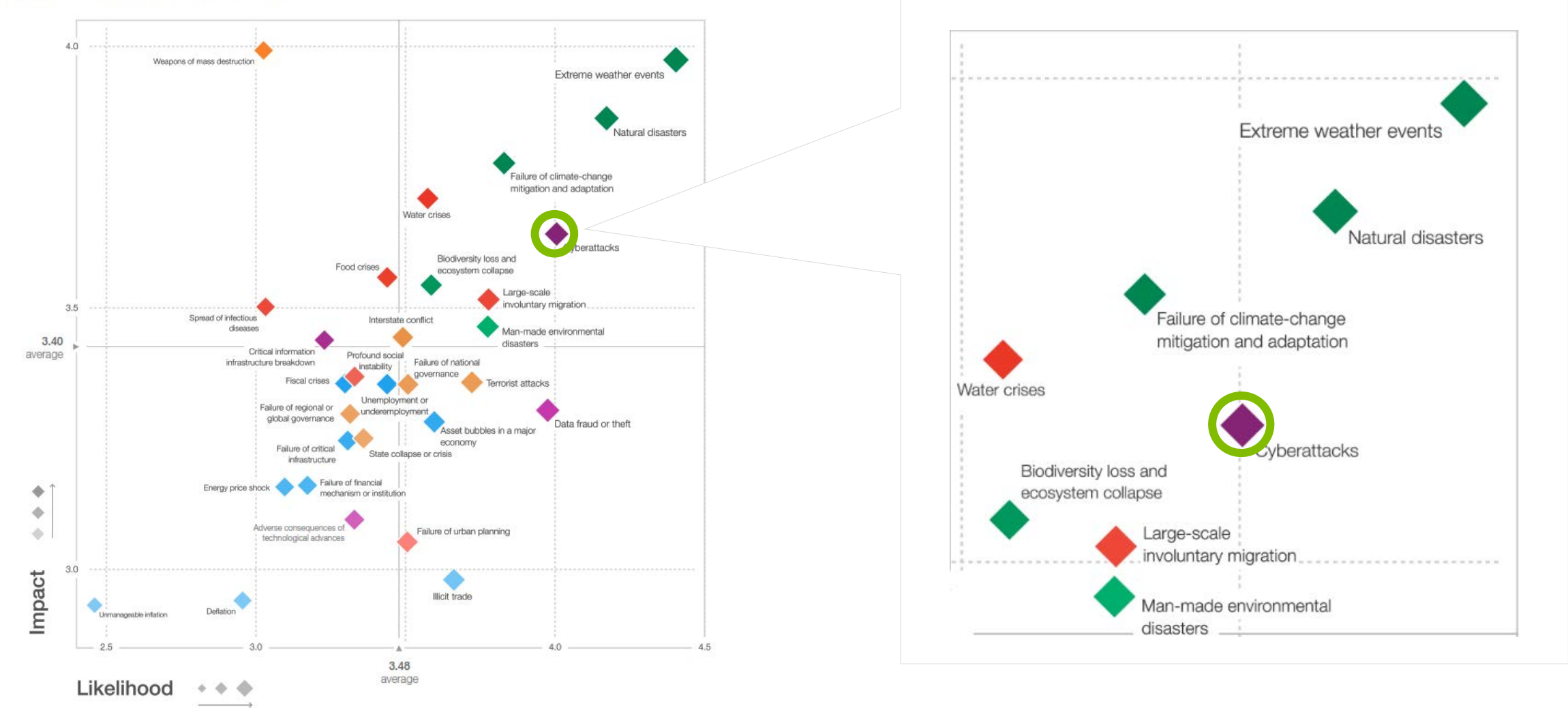
The Changing Nature of Relationships

- State – Citizen
- Enterprise – Enterprise & Gov't
- Government – Government
- Enterprise – Consumer
- Enterprise – Enterprise
- Citizen – Citizen

The Digital Revolution

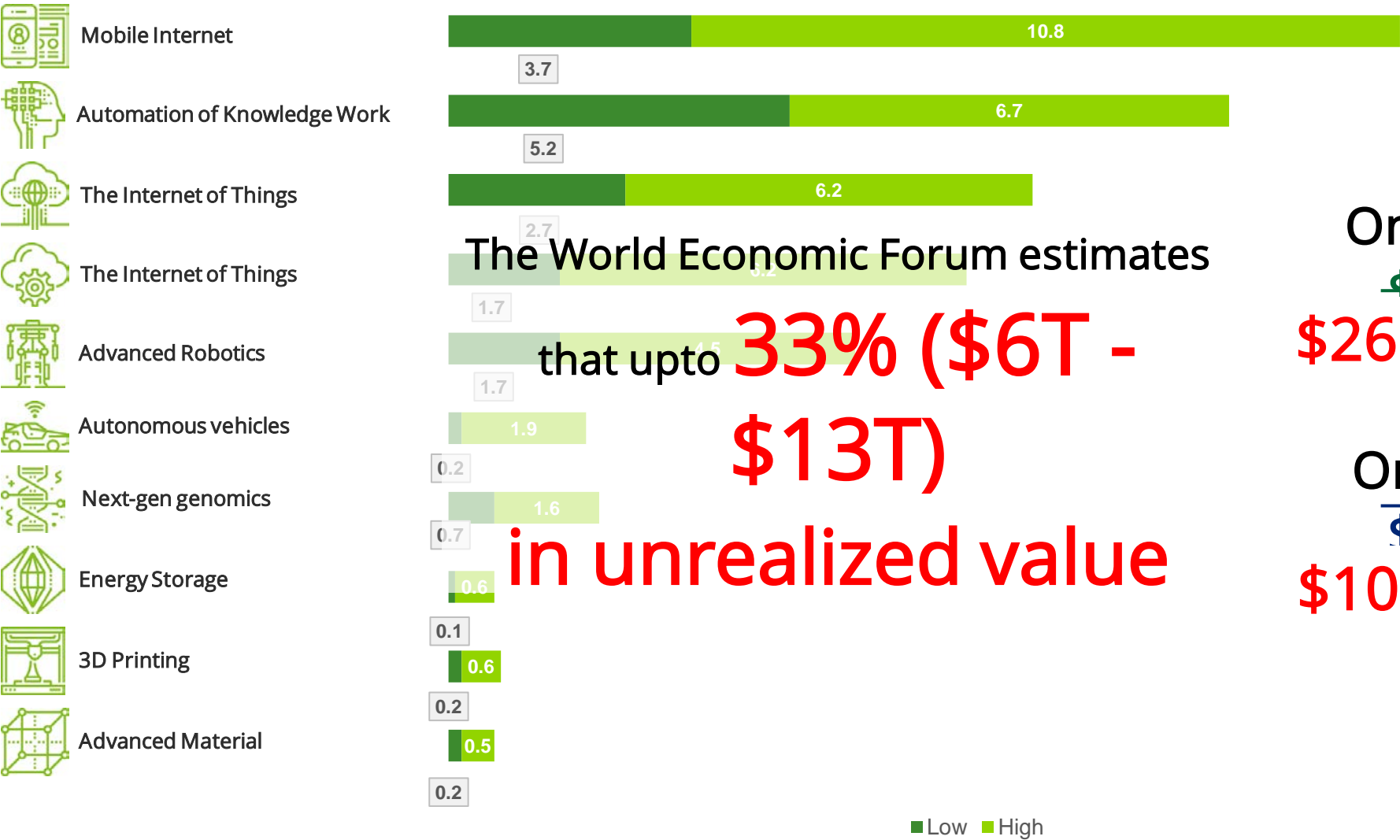
World Economic Forum – Top Global Risk - 2018

Figure I: The Global Risks Landscape 2018



The Digital Revolution

Estimated economic impact of technologies in 2025 (\$ Trillions)



The World Economic Forum estimates
that upto **33% (\$6T - \$13T)**
in unrealized value

On the High End
~~\$20.6 Trillion~~
\$26.1 Trillion USD

On the Low End
\$16.4 Trillion
\$10.8 Trillion USD

The Global Threat Landscape

Cyber threat continues to increase in scale and sophistication at an extraordinary rate. At one time, the most advanced cyber-attack tools and methods were restricted to a small handful of national players; now, more actors than ever, including nation state actors and organized criminal enterprises, are developing highly-skilled resources and capabilities, or acquiring them through an expanding black market for illicit activities.

The Global Threat Landscape

Cyber Crime Statistics



≈ 80B

Daily Malicious Scans



≈ 300K

New Malware Been Created Daily



≈ 780K

Records Lost to Hacking Daily

The Major Motivation Behind Cyber Attacks

76.5%

Cyber Crime

19.4%

Cyber Espionage

3.1%

Cyber Warfare

1%

Hacktivism

Top 3 Industries Attacked in 2017



Financial
Services
25%



Retail
13%



Health Care
19%



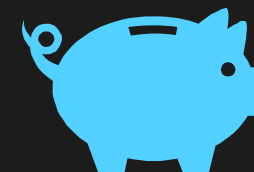
2017 Estimated Annual Total
Cost of Cyber Crime

≈ \$600B



2017 Avg per Capita Cost
per Data Breach

≈ \$155



2017 Avg Total Cost
(Indirect / Direct) of Data Breach

≈ \$4.94M

* Statistics provide by IBM 2015 Cyber Security Intelligence Index Report & Ponemon Institute - 2016 Cost of Data Breach Study: Global Analysis



While many organizations now **recognize that cyber risk is a top business risk**, despite the heightened attention the number of cyber incidents and their associated costs continues to rise.

The Global Threat Landscape

Most Notable Attacks of 2017

Jan 2017, Saudi state-run TV reported that 15 government agencies and organizations had been hit with Shamoon 2 wiping data and taking control of the computer's boot record, which prevented the PC from being turned back on

May 2017, WannaCry, which spanned more than 150 countries, leveraged some of the leaked NSA tools. The ransomware targeted businesses running outdated software and locked down computer systems. The hackers behind WannaCry demanded money to unlock files. More than 300,000 machines were hit across numerous industries,

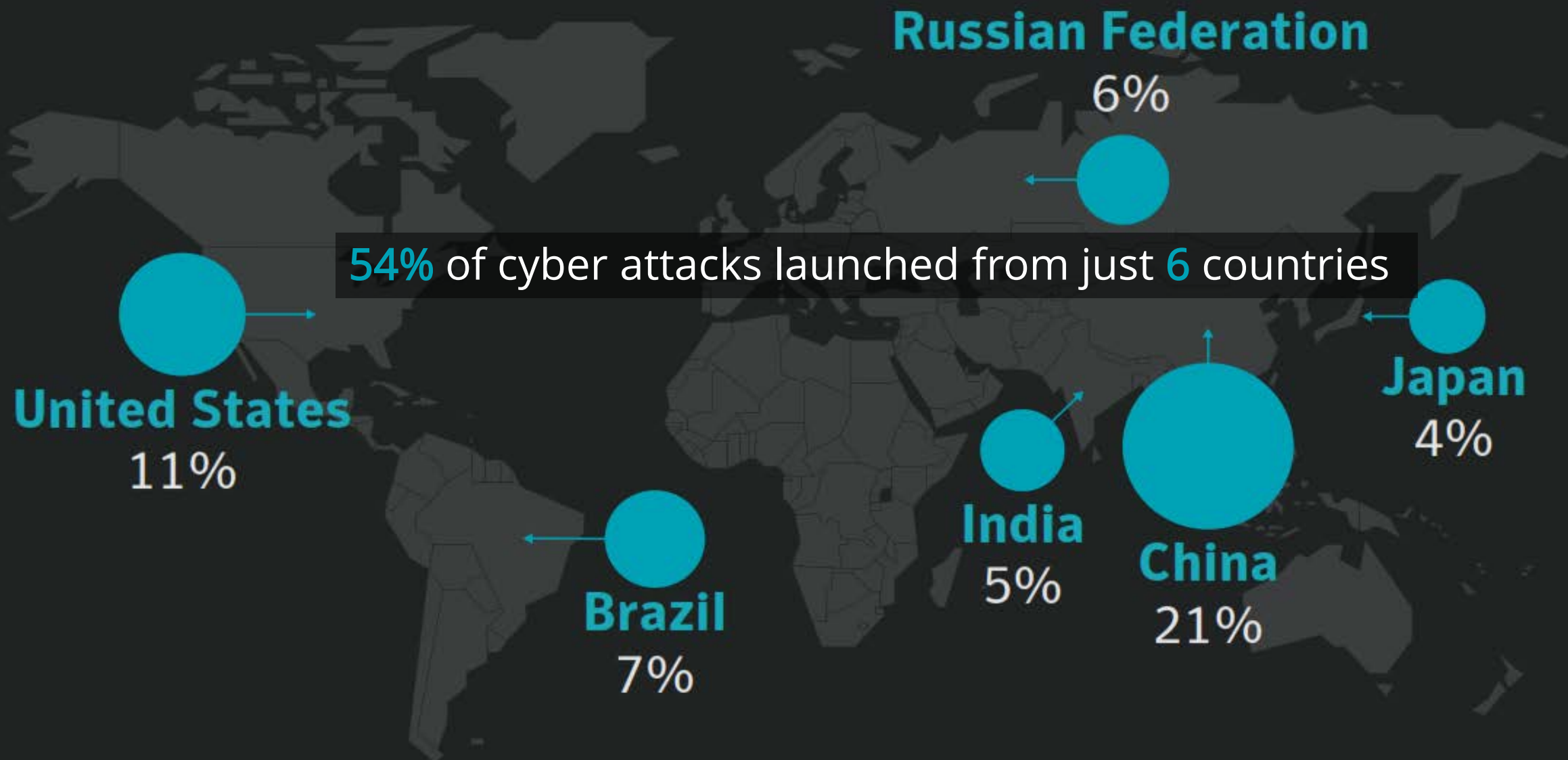
July 2017, a large credit bureau was penetrated by cybercriminals in July and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including Social Security numbers.

April 2017, an anonymous group called the Shadow Brokers leaked a suite of hacking tools widely believed to belong to a government security agency. The tools allowed hackers to compromise a variety of Windows servers and Windows operating systems, including Windows 7 and Windows 8.

April 2017, the computer virus NotPetya targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses. This virus also spread by leveraging a vulnerability leaked by the Shadow Brokers. In September, FedEx attributed a \$300 million loss to the attack. The company's subsidiary TNT Express had to suspend business.

The Global Threat Landscape

Attack Origins



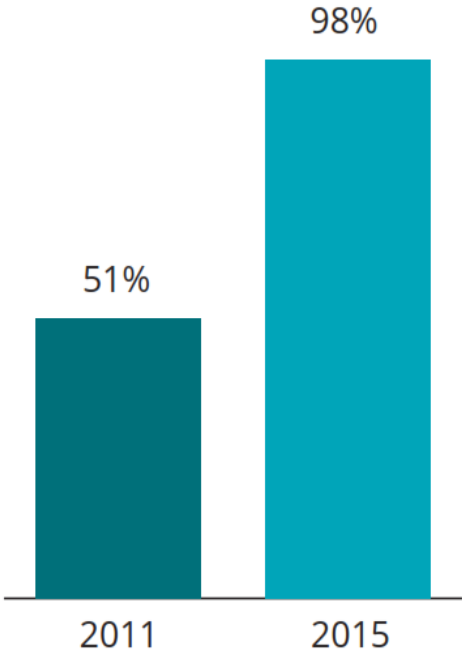
The Evolving Threat Landscape

Lessons Learned from the Front Lines

How **secure** is the system?



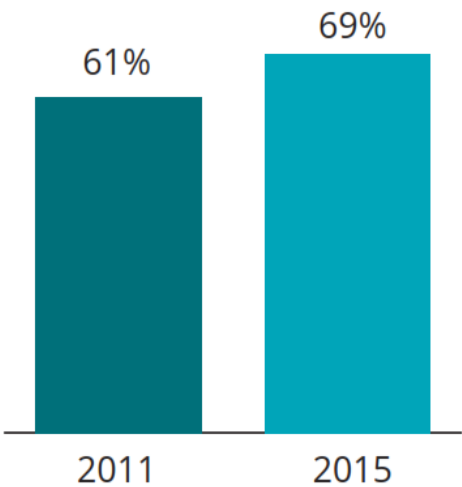
The time it took attackers to **compromise** the system from the start of the attack:
Incidents within minutes or less*



How **vigilant** is the system?



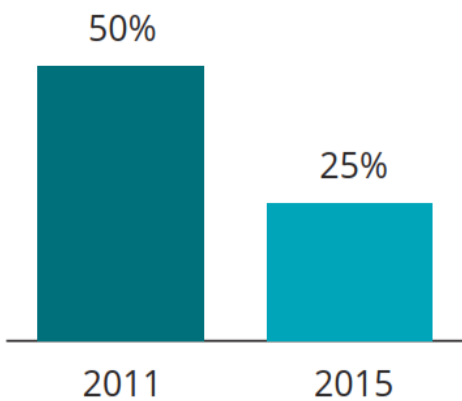
The time it took victims to **discover** the incident:
Incidents took weeks or more



How **resilient** is the system?

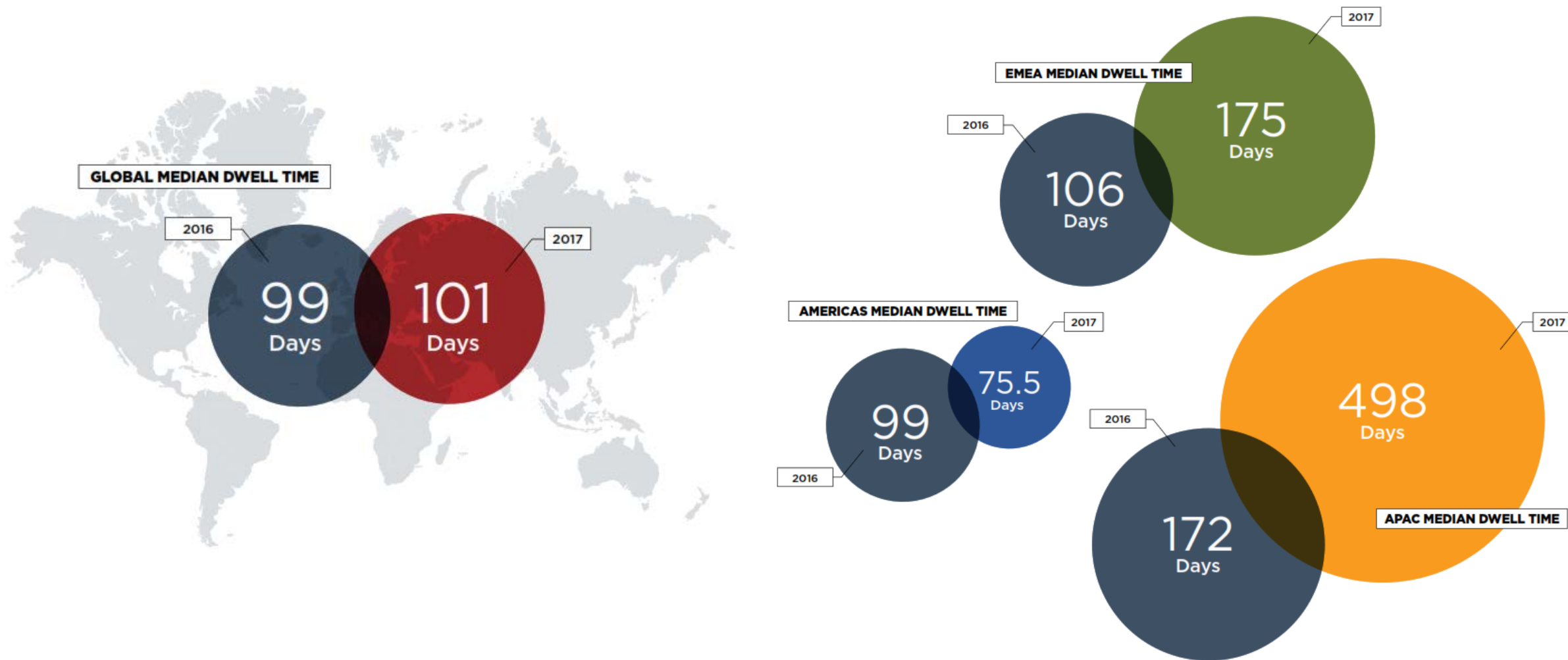


The time it took victims to **contain** the incident:
Incidents took weeks or more



The Evolving Threat Landscape

Median Dwell (Time to Identify Attack) Time



The Current Threat Landscape

The Middle East on High Alert

In addition to the current global cyber threat landscape, the **Middle East faces 3 unique dimensions of risk** which translates in to an elevated level of cyber threat that must be considered.

Regional Geo-Political Instability



Since 2010 the Middle East has seen significant Geo-Political instability which has given rise to various hacktivist groups. These hacktivist groups have reigned cyber havoc on governments, public and private institutions in the region on almost a daily basis since the inception of the turmoil.

Perceived Economic Wealth



The Middle East in the eyes of the global community is perceived as a region of economic wealth. To cyber criminals who are trying to exploit governments, public and private institutions for financial gains this makes the Middle East a central target for attack and indeed has been.


Significantly Higher than Average Infection Rates



Microsoft, since 2012 has published a quarterly report on the average malware infection rate per country including a global average. Without exception every country in the Middle East has had at least double (in some cases twenty times the global average) the number of infected systems per quarter than the global average.

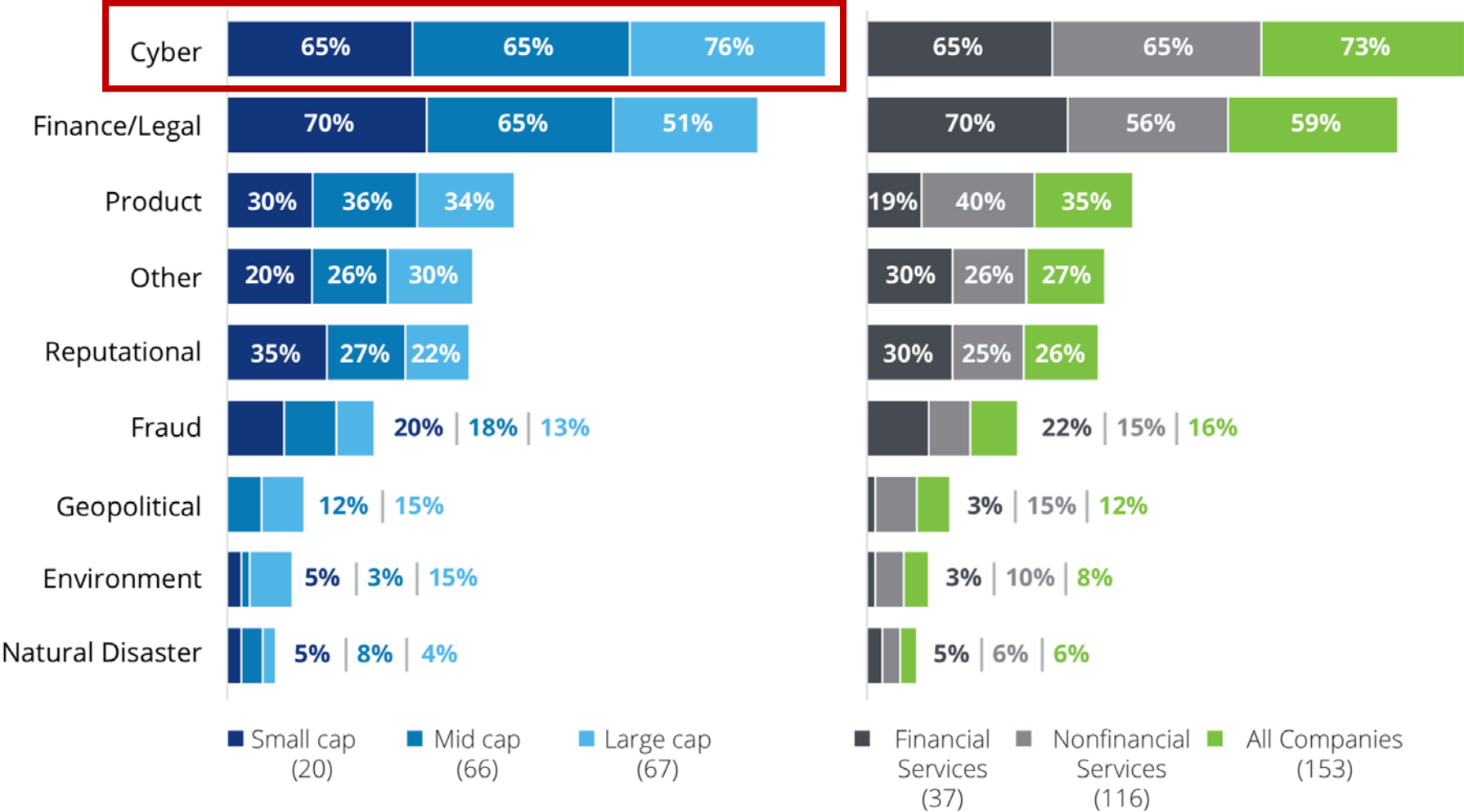


Despite the increased **recognition that cyber risk is a top business risk** and a 7.8% year-over-year increase in average spend on cyber security, **why are organizations still struggling to manage cyber risk?**



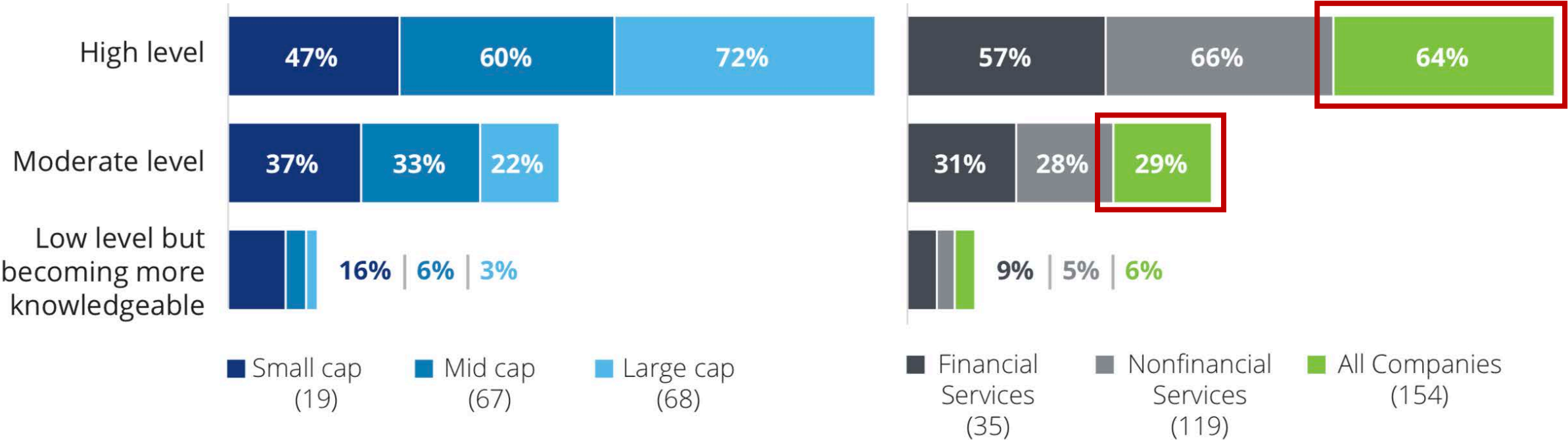
A recent survey conducted by Deloitte's Center for Board Effectiveness and the Society for Corporate Governance (Society) examines **the current practices of boards related to cyber security and also offers some insight into the current challenges related to cyber security governance:**

Rank the top three risks that your board is focused on



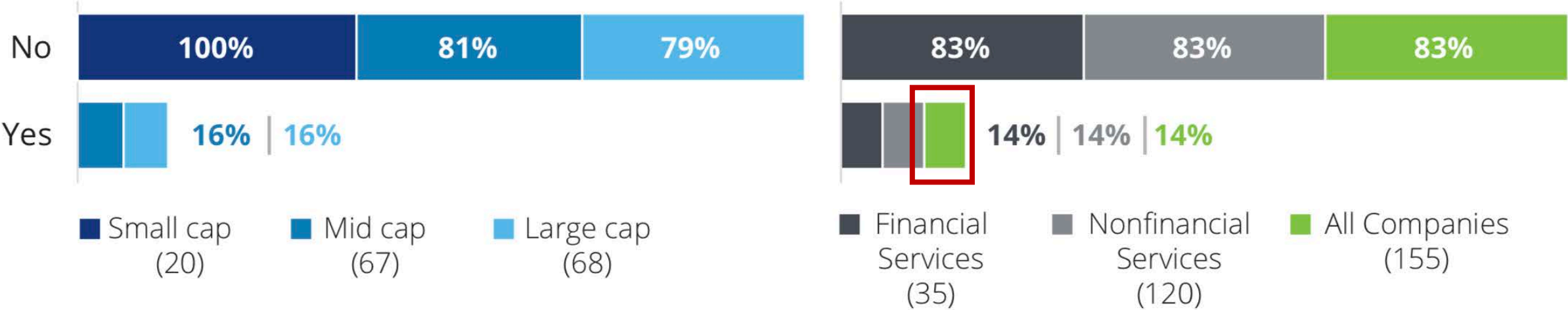
A majority of boards’ directors at large cap organizations have indicated that cyber risk is the top risk that as a board, are focusing on.

What level of awareness specific to your company does the board have on cyber security?



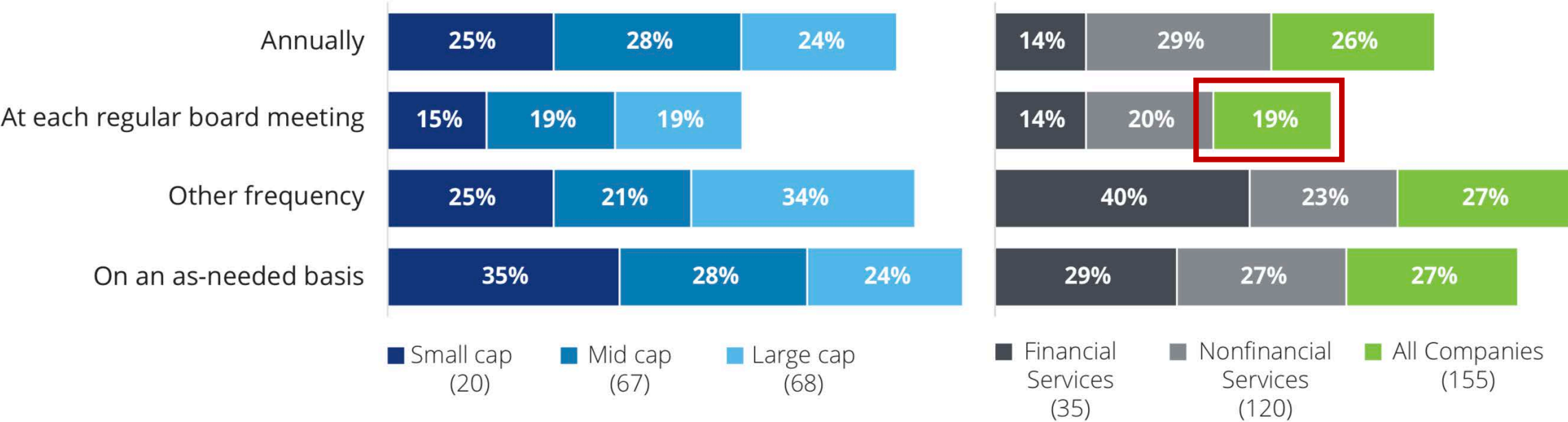
64% of boards have a high level of awareness of cyber security, and 29% have a moderate level of awareness confirming the notion that the level of cyber security awareness at the board level is high.

Have you added a director with cyber experience to your board in the past two years?



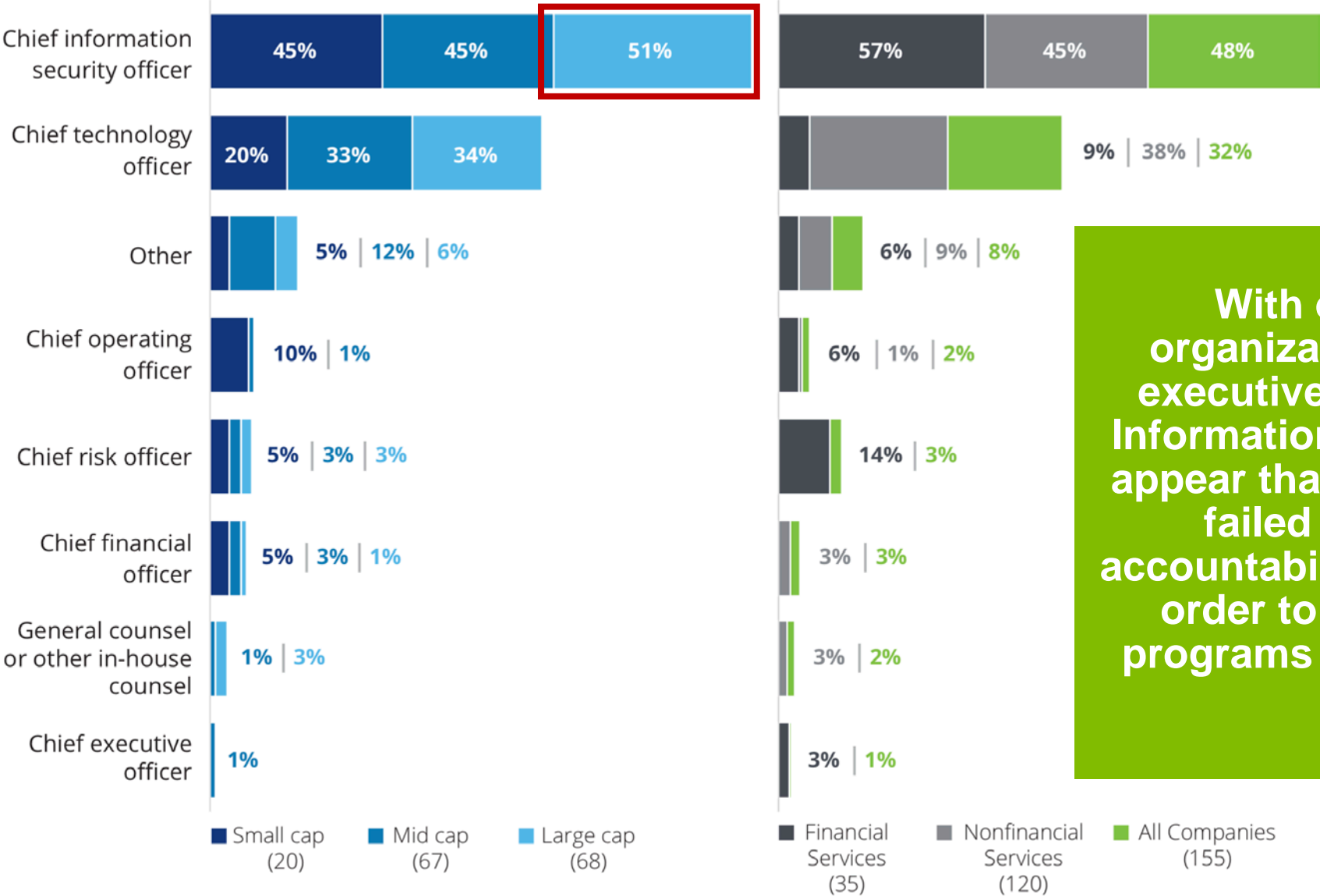
Despite 14% of boards having added a board member with cyber experience in the past two years a resounding majority of boards still sit without one and while awareness is a vital first step of strong corporate governance, safeguarding an organization’s crown jewels requires accountability and timely action. Could the absence of a board member with specialist technology or cyber background be one of the factors contributing to why cyber security programs are failing?

How often does the board receive reports on cybersecurity?



The cyber threat landscape is ever changing and voluminous. With only 19% of boards receiving updates at each regular board meeting, are board of directors being sufficiently kept up to date on the current state of the organization’s cyber security capabilities? And subsequently can actions be taken quickly enough in order to manage that risk within acceptable levels?

Who is responsible for reporting on cybersecurity to the board?



With only 51% of large cap organizations having a dedicated executive for cyber security (Chief Information Security Officer) it would appear that many organizations have failed to establish sufficient accountability at the executive level in order to drive the cyber security programs required to manage cyber risk.



As with all things governance **“tone-from-the-top” is key**, cyber security governance is no different.

Cyber Security Governance

Results of the Survey & Characteristics of an Effective Program

What the survey seems to indicate, is that **there is still a divide when it comes to translating that cyber risk awareness into organizational specific understanding and subsequent action.**

Organizations that govern and manage cyber security well have a few common characteristics:

- ❖ Management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
- ❖ Management incorporates risk-informed decision making into day-to-day operations, and fully integrates risk management into operational processes
- ❖ The board, walks a fine line, playing an active role in oversight, but not extending itself into the day-to-day management of the business is fully aware of internal and external threats, and proactively provides direction and guidance to the management allowing for agile response to changes in threat.

Cyber Security Governance

Boards of Directors can focus on the following leading practices:

- 1. Become aware of cyber threats:** Whether or not there is a dedicated risk committee on the Board, it is important to have directors with knowledge and skills pertaining to security, IT governance and cyber fraud.
- 2. Coordinate cyber threat initiatives:** In its capacity of overseeing risk management activities and monitoring the management's policies and procedures, the Board plays a strategic role in coordinating cyber risk initiatives and policies, and confirming their efficacy
- 3. Appoint a senior management person to develop a cyber-threat response plan:** It is recommended that the Board appoint an executive, focused on information security, so that there is a clear voice directing cyber threat prevention, remediation and recovery plans, related educational activities, and the development of frameworks for effective reporting.
- 4. Leverage external specialists to review cyber-threat response plans:** External specialists can often be a valuable source of information on cyber security issues for evaluating and strengthening security controls and implementing programs for cyber risk management.
- 5. Evaluate the effectiveness of the cyber security program:** Boards and C-suites must ensure that the cybersecurity program is reviewed for effectiveness and that any identified gaps are appropriately managed in line with risk appetite.
- 6. Prepare for the inevitable:** The board should hold management accountable for implementing a cyber crisis management plan and for building cyber resilience capabilities that address the unique risks to the organization.



Thank You

Q&A



© 2016 Deloitte & Touche (M.E.)

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte & Touche (M.E.) is a member firm of Deloitte Touche Tohmatsu Limited (DTTL) and is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926.

Deloitte provides audit, tax, consulting, and financial advisory services through 26 offices in 15 countries with more than 3,300 partners, directors and staff. It is a Tier 1 Tax advisor in the GCC region since 2010 (according to the International Tax Review World Tax Rankings). It has also received numerous awards in the last few years which include best employer in the Middle East, best consulting firm, the Middle East Training & Development Excellence Award by the Institute of Chartered Accountants in England and Wales (ICAEW), as well as the best CSR integrated organization.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.