KPMG

Cybersecurity Total Protection

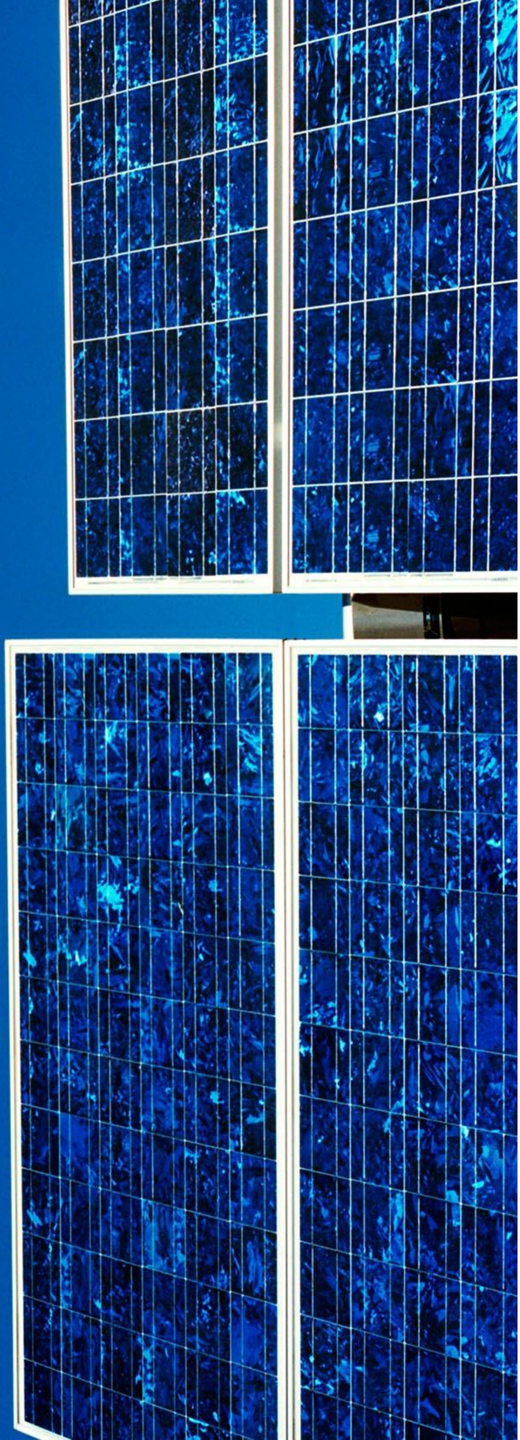
May 1, 2017

Introduction

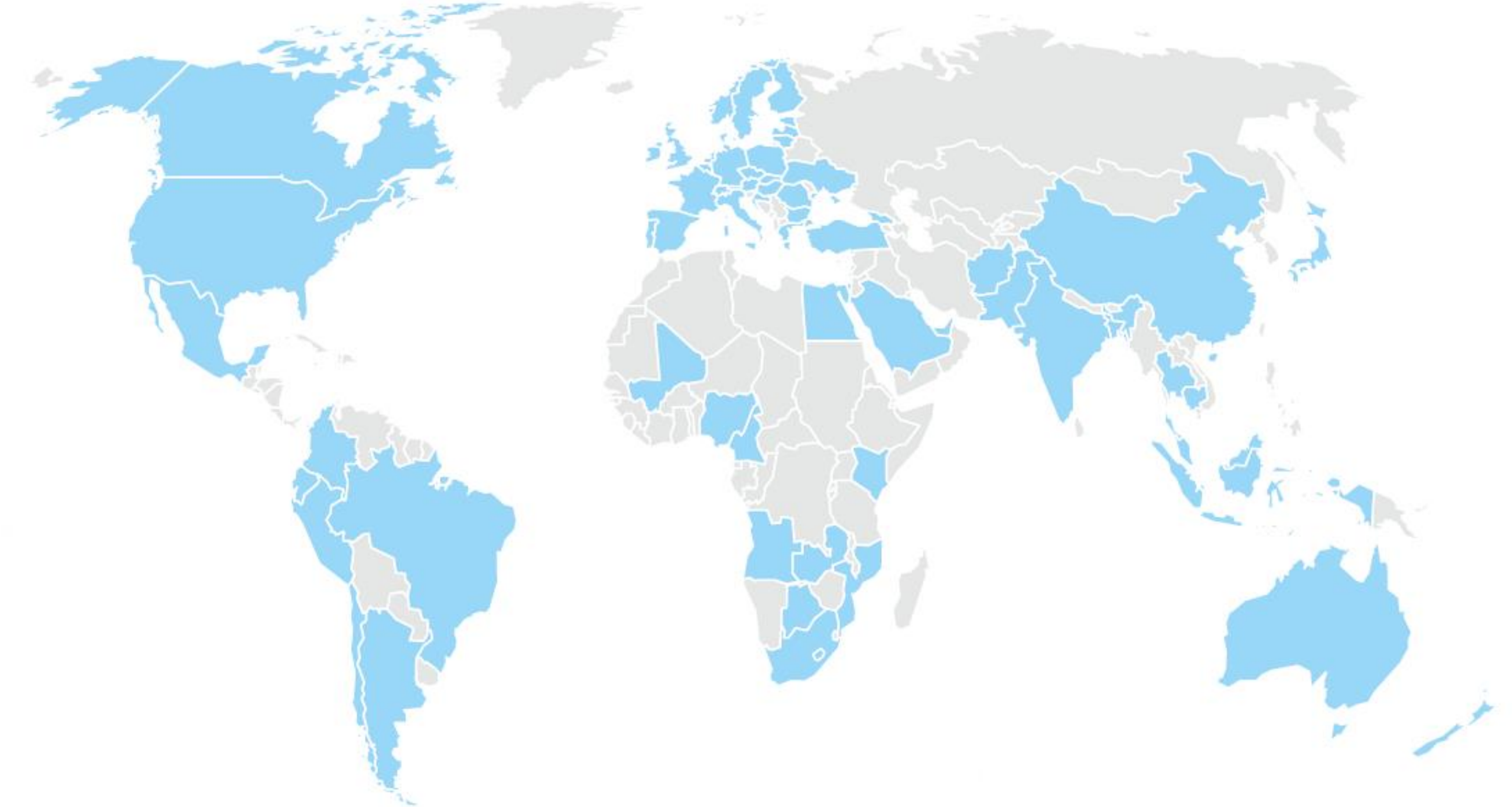
Manhal M. Musameh

Head of IT Advisory

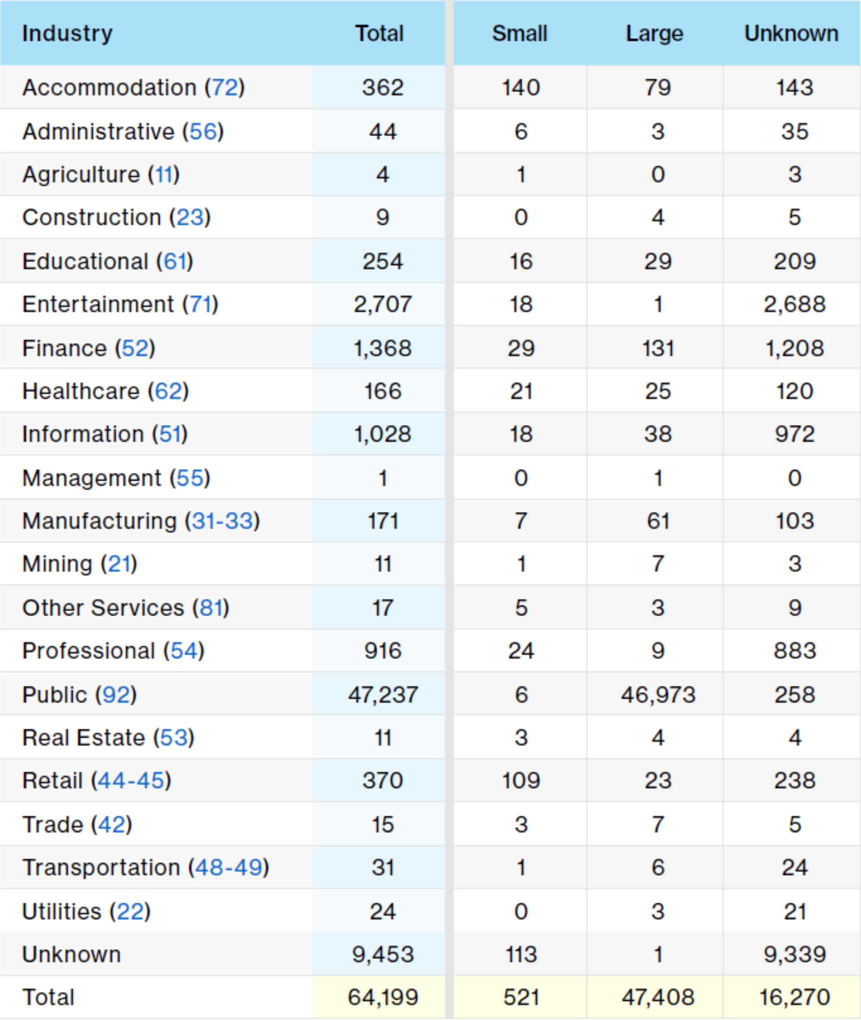
KPMG Al Fozan and Partners



Incidents landscape

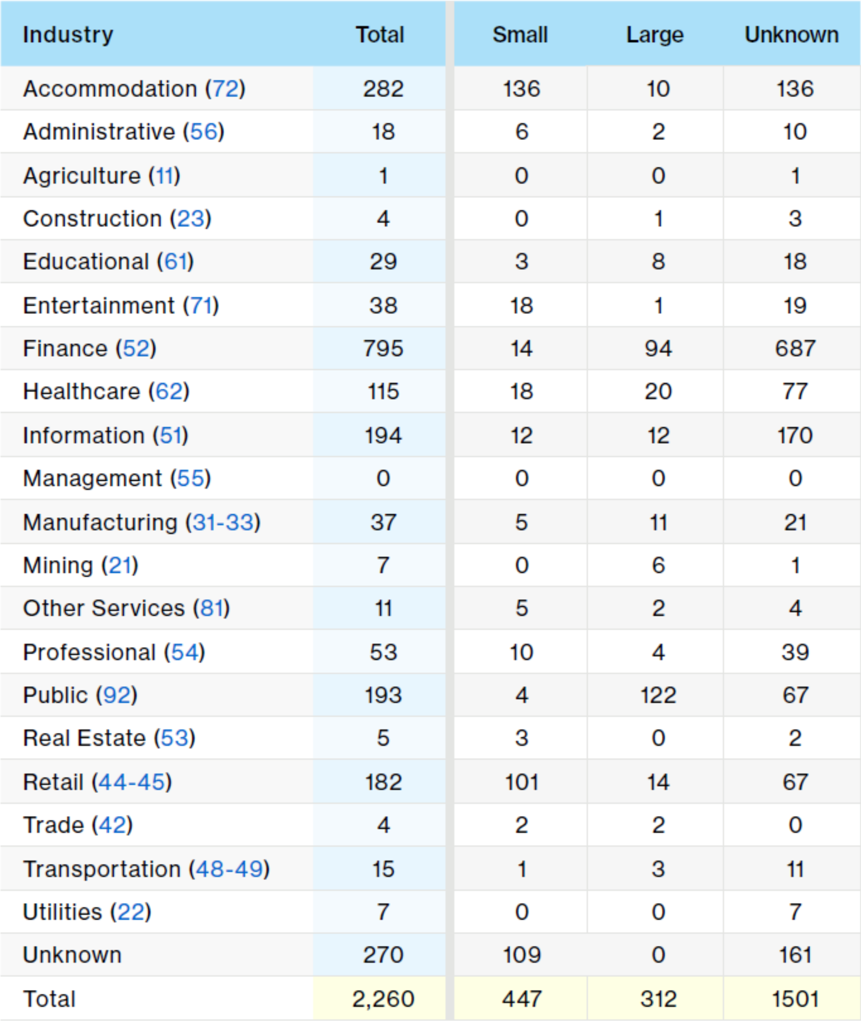


Number of security incidents



Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

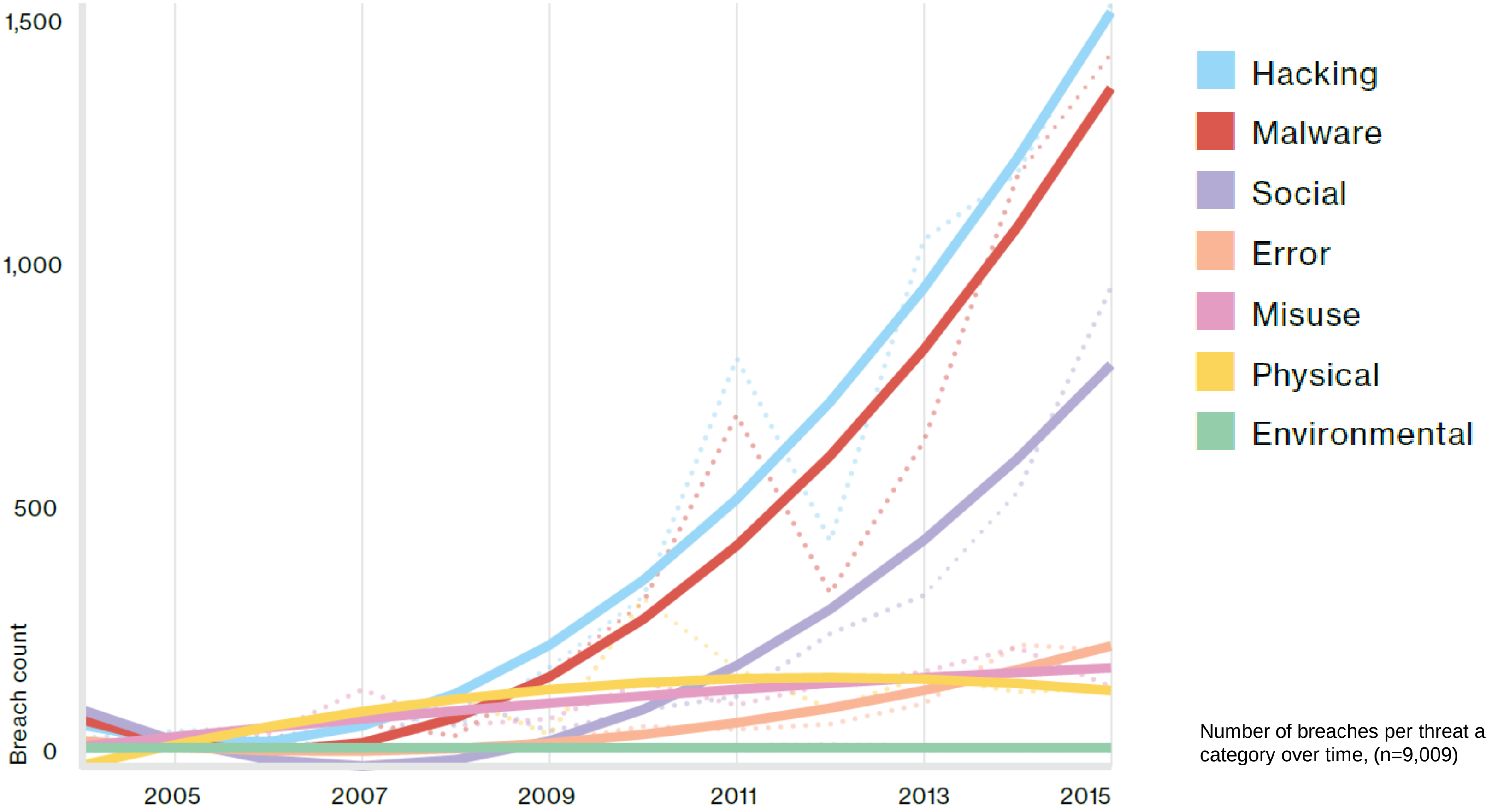
Number of security incidents by victim industry and organization size, 2015 dataset.



Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	182	101	14	67
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Number of security incidents with confirmed data loss by victim industry and organization size, 2015 dataset.

Number of breaches per threat action category over time



Number of breaches per threat action category over time, (n=9,009)

What is Information Security?

Information Security NIST Definition:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

SOURCE: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542

Information Security NIST Definition:

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

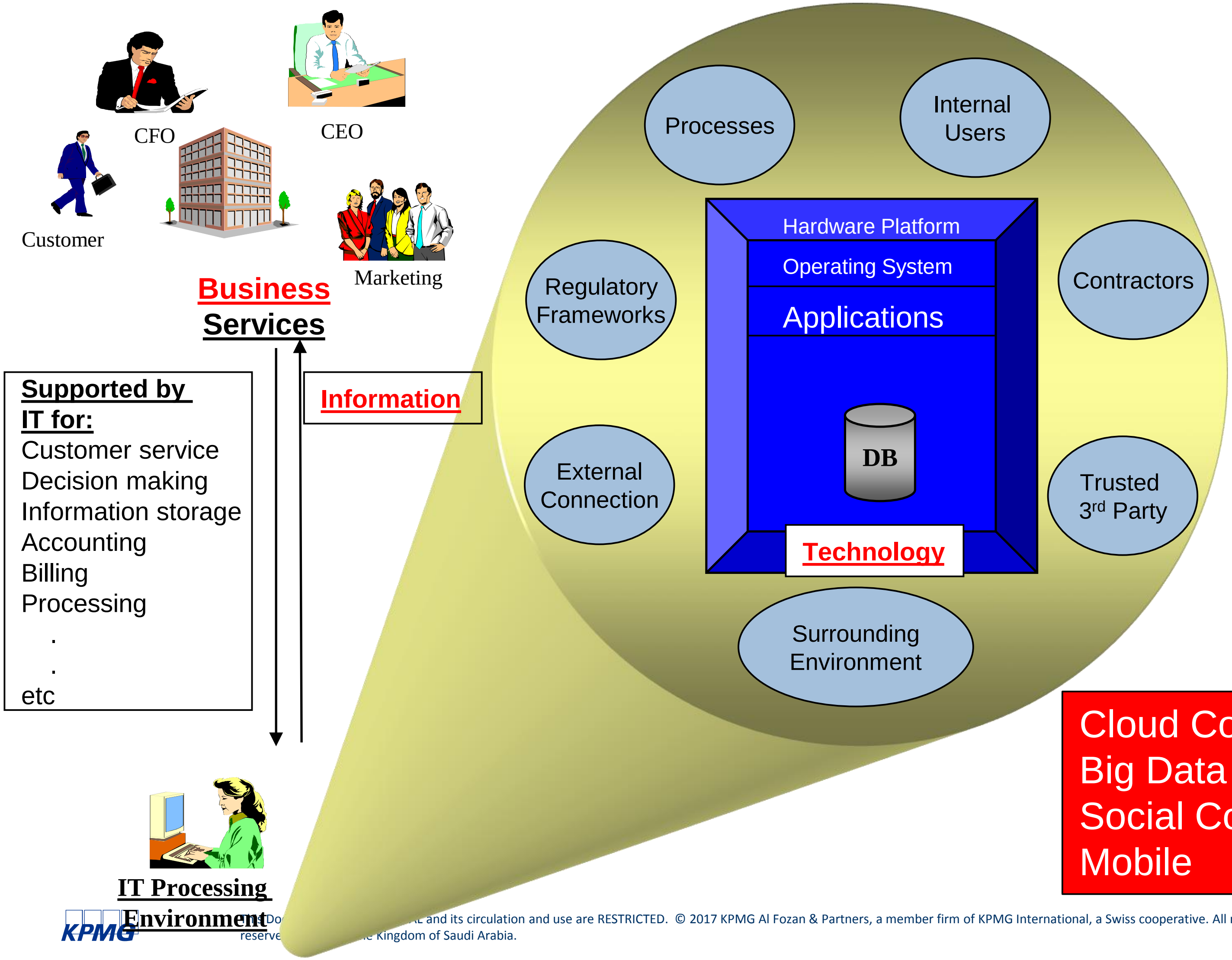
3. Availability, which means ensuring timely and reliable access to and use of information

SOURCE: SP 800-66; 44 U.S.C., Sec 3541

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Information Security is about Trust and Protection

Business - Information - Technology



Supported by IT for:
Customer service
Decision making
Information storage
Accounting
Billing
Processing
.
.
etc

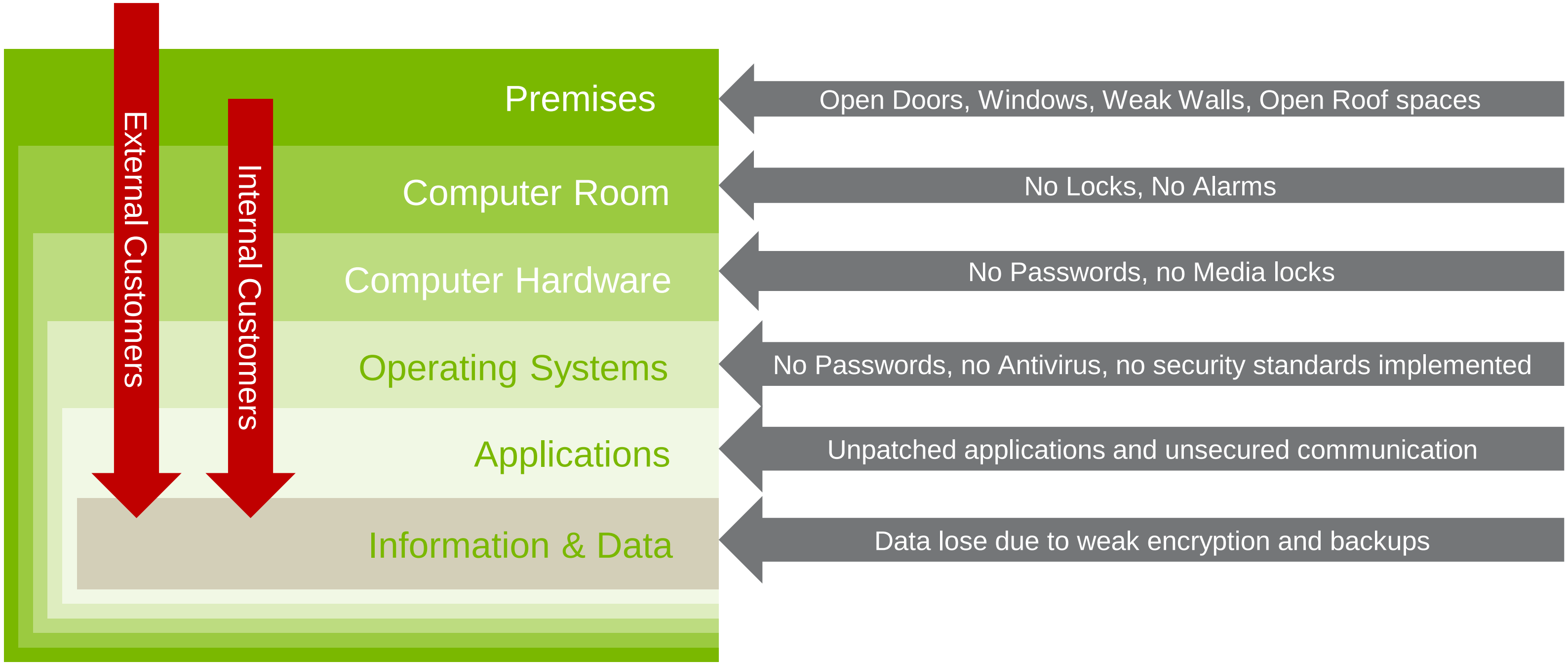
Threats:

- Internal attacks
- External attacks
- Human errors
- Data misuse
- System errors
- Viruses
- Hardware failure
- Physical damage
- Natural disasters

Cloud Computing
Big Data
Social Collaboration
Mobile

Classical Security Layers

Security is all about protection layered in depth through the provision of barriers to access. Different layers of protection must be built around important equipment and information. The following access must be protected:


External Customers
Internal Customers
Premises
Open Doors, Windows, Weak Walls, Open Roof spaces
Computer Room
No Locks, No Alarms
Computer Hardware
No Passwords, no Media locks
Operating Systems
No Passwords, no Antivirus, no security standards implemented
Applications
Unpatched applications and unsecured communication
Information & Data
Data lose due to weak encryption and backups

Information Security Controls

Access Level

Customer

Customers

- Educate your employees
- NDAs and Confidentiality Agreements
- Unique IDs
- Establish strong passwords

Delivery Chanel

Mobile Access

Web Access

Service Desk

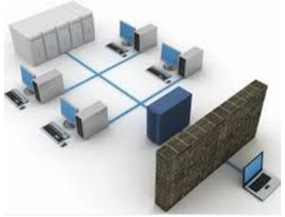
ATM Access

- Secure your laptops
- Secure your mobile phones
- Educate your Service Desk Support

Application & Data

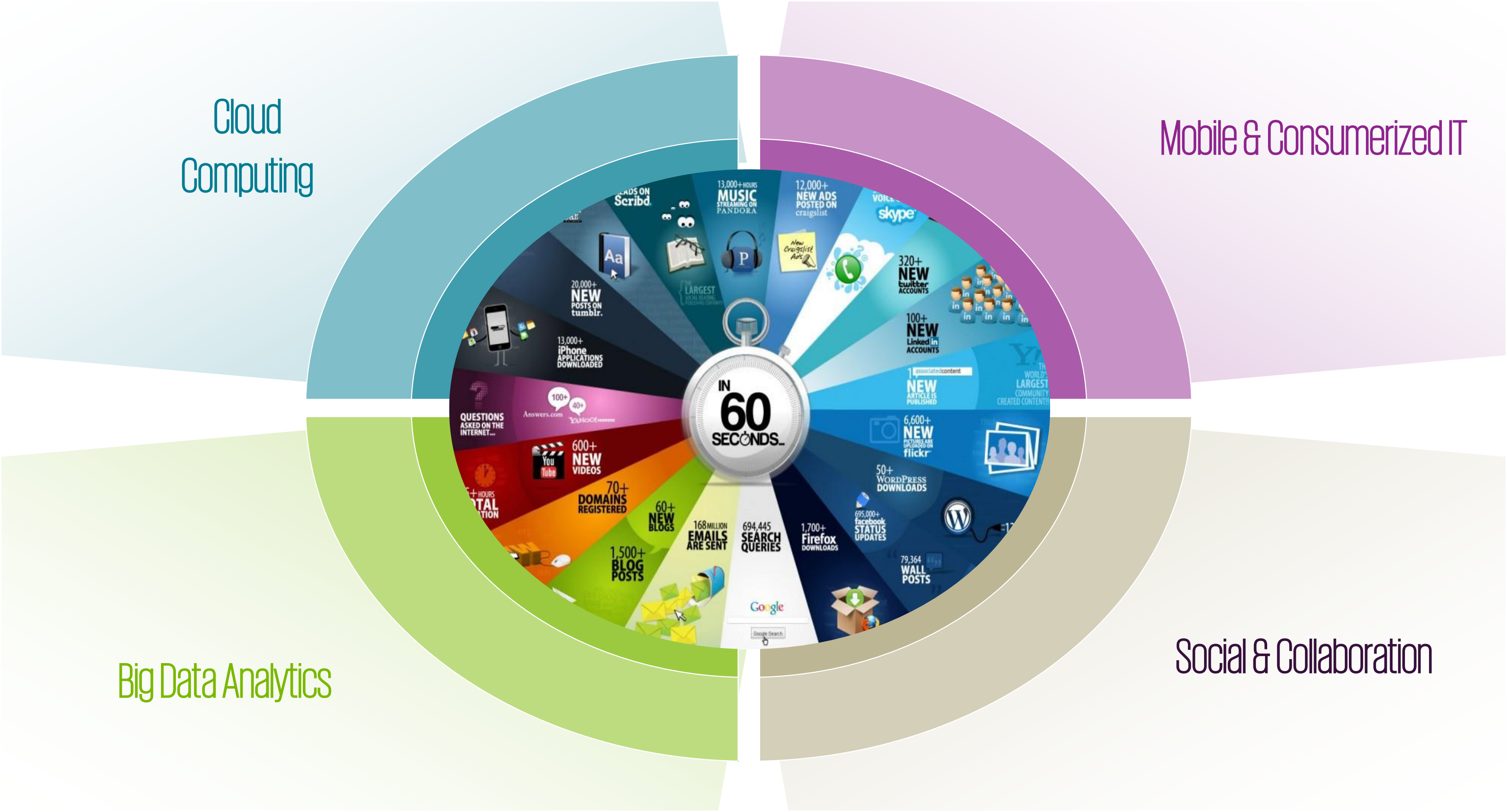
- Update your programs regularly
- Backup regularly
- Install antivirus protection
- Educate your system and Database Admins

Technology



- Protect the network
- Protect the Site
- Monitor diligently
- Educate your Engineers

Digital tsunami Is Coming …



Cloud Computing

Mobile & Consumerized IT

Big Data Analytics

Social & Collaboration

IN 60 SECONDS...
ADS ON Scribd
THE LARGEST SOCIAL READING PUBLISHING COMPANY
13,000+ HOURS MUSIC STREAMING ON PANDORA
12,000+ NEW ADS POSTED ON craigslist
New Craigslist Ads
VOICE skype
320+ NEW twitter ACCOUNTS
100+ NEW LinkedIn ACCOUNTS
1 associatedcontent NEW ARTICLE IS PUBLISHED
THE WORLD'S LARGEST COMMUNITY CREATED CONTENT
6,600+ NEW PICTURES ARE UPLOADED ON flickr
50+ WORDPRESS DOWNLOADS
695,000+ facebook STATUS UPDATES
79,364 WALL POSTS
1,700+ Firefox DOWNLOADS
694,445 SEARCH QUERIES
Google
Google Search
168 MILLION EMAILS ARE SENT
1,500+ BLOG POSTS
60+ NEW BLOGS
70+ DOMAINS REGISTERED
600+ NEW VIDEOS
You Tube
+ HOURS TOTAL DURATION
QUESTIONS ASKED ON THE INTERNET...
100+ Answers.com
40+ YAHOO! ANSWERS
13,000+ iPhone APPLICATIONS DOWNLOADED
20,000+ NEW POSTS ON tumblr.
Aa
P

These new technologies propels us into a 'Digital World' that demands organizations to adapt to new economic models, structures and behaviour

Digital Technologies

New technologies: 'omni-present'

New technologies enable mass-customization, flexible value chains, open exchange of data and working any time, any place, anywhere

Digital World

New economy; '24/7, faster heartbeat'

New economies emerge, driven by rapid, often customer driven changes, shorter lifecycles of products & services (information- / network economy), 24/7

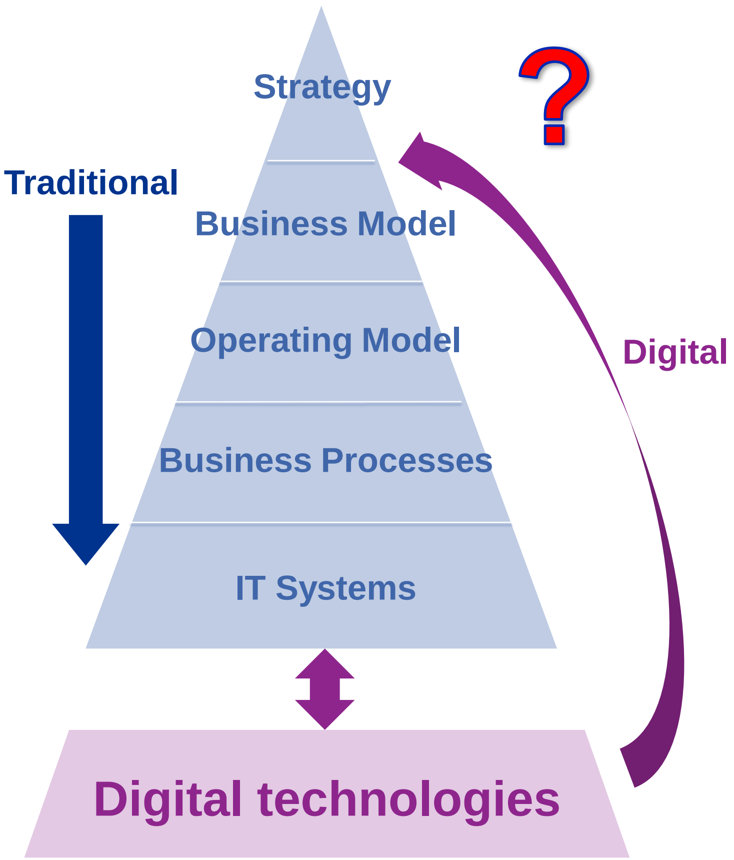
New organisation; 'blurred lines'

The traditional, stable organisation model becomes irrelevant, due to technology driven break-down of barriers and availability of (open) information

New human behaviour; 'tech-savvy'

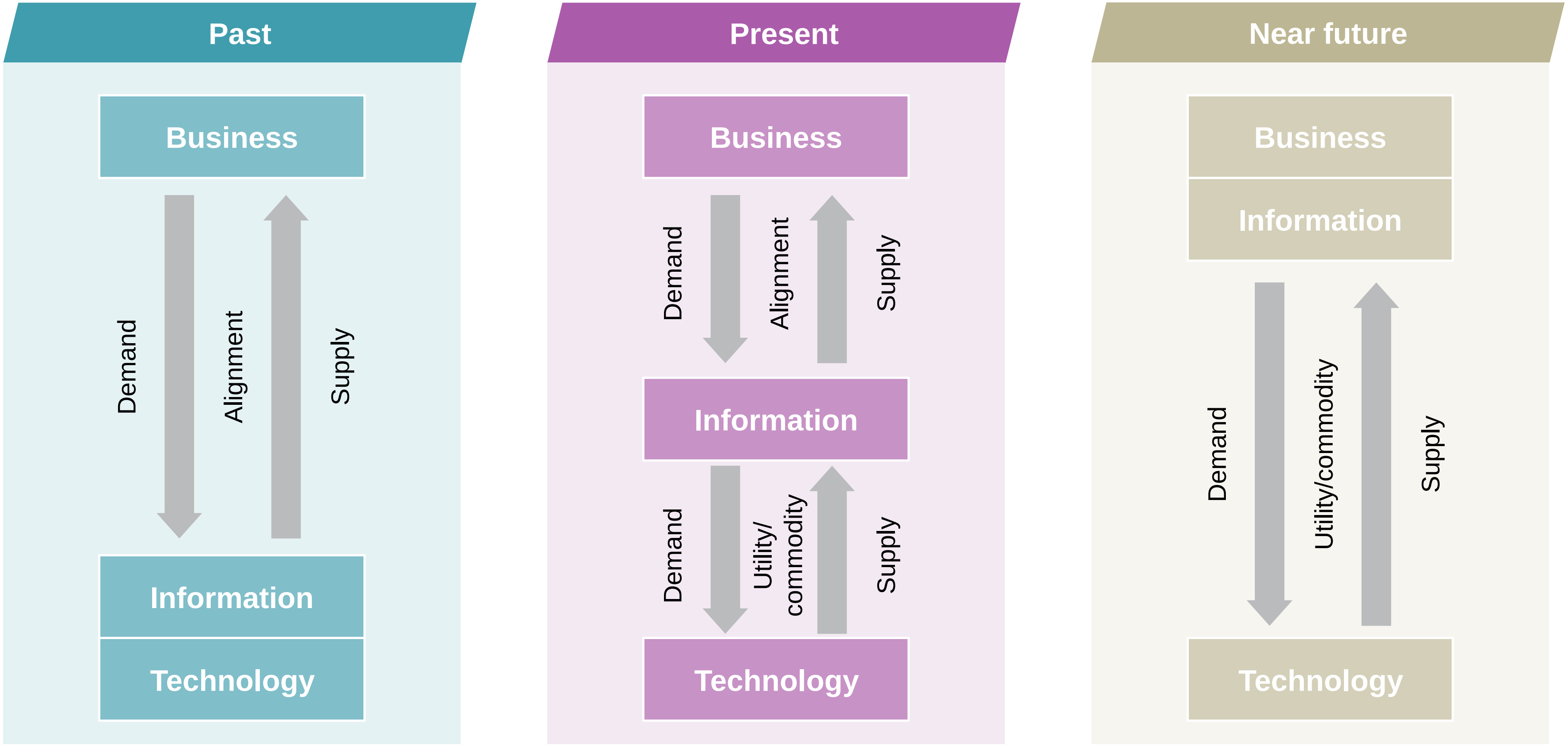
A new generation of people is arriving, that is used to instant availability of (open) information, user defined functionality, in the palm of their hands at any time

But in order to survive, organizations and their CIOs need to realize that a digital world requires a differentiated approach towards their IT



	‘Traditional’ IT	Digital
Strategy	Translate business function demands into what IT needs to deliver	Use possibilities from digitized technologies to continuously innovate the business model
Role	Reactive supporter	Proactive advisor
Support	Operational functions	Customers
Triggers	Internal	External
Speed	Slow	Fast
Process	Planning	Learning
Projects	Large Transformations	Small Proofs of Concept
IT Roles	Plan / Build / Run	Broker / Integrate / Orchestrate
IT Systems	Systems of record	Systems of engagement
External	Vendors	Partners
Result	**Business as usual**	**Business as UNusual**

Eventually the business will (re)take ownership of information, enabling business processes with easy-to-use technology



Technology will be become more advanced, but easier to use

Internet of Things

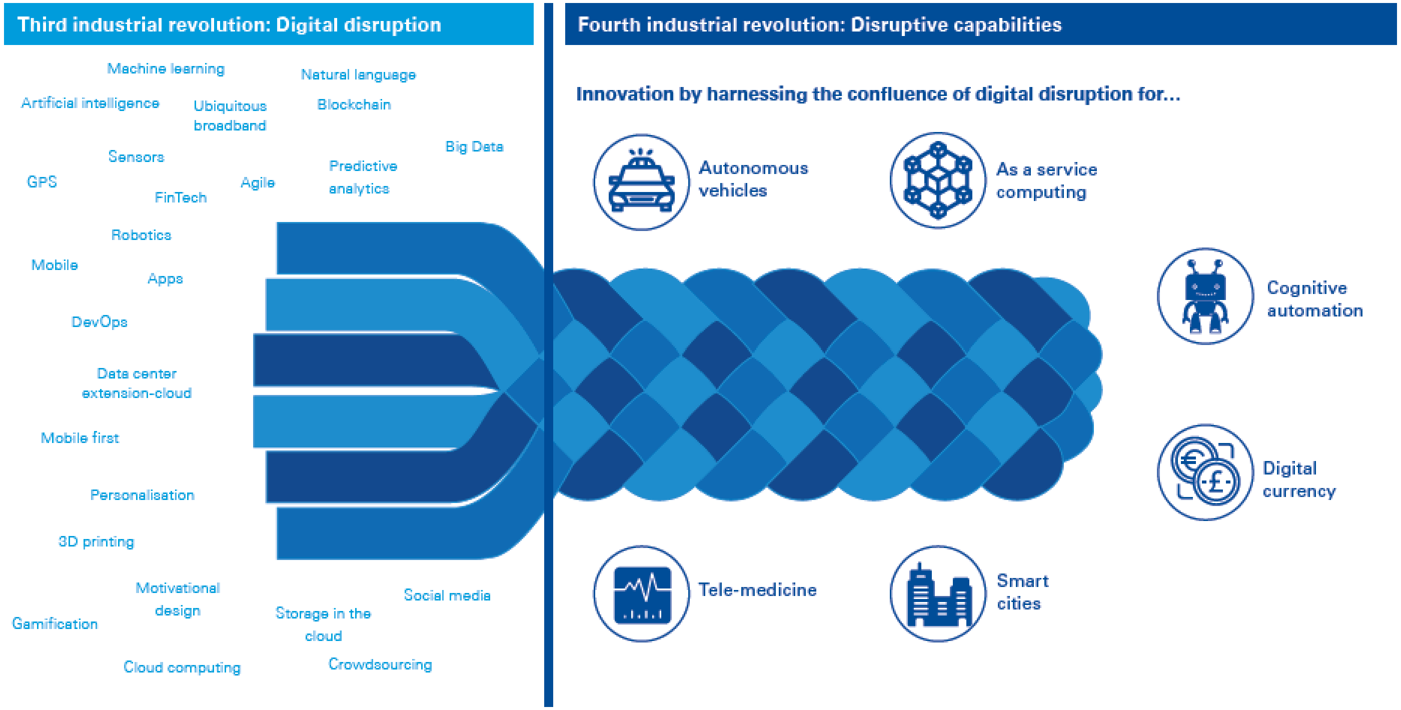
Smart Life

Smart Mobility

Smart City

Smart Manufacturing

The unlimited disruptive capabilities



Third industrial revolution: Digital disruption

Machine learning
Natural language
Artificial intelligence
Ubiquitous broadband
Blockchain
Big Data
Sensors
Predictive analytics
GPS
Agile
FinTech
Robotics
Mobile
Apps
DevOps
Data center extension-cloud
Mobile first
Personalisation
3D printing
Motivational design
Social media
Gamification
Storage in the cloud
Cloud computing
Crowdsourcing

Fourth industrial revolution: Disruptive capabilities

Innovation by harnessing the confluence of digital disruption for…

Autonomous vehicles
As a service computing
Cognitive automation
Digital currency
Tele-medicine
Smart cities

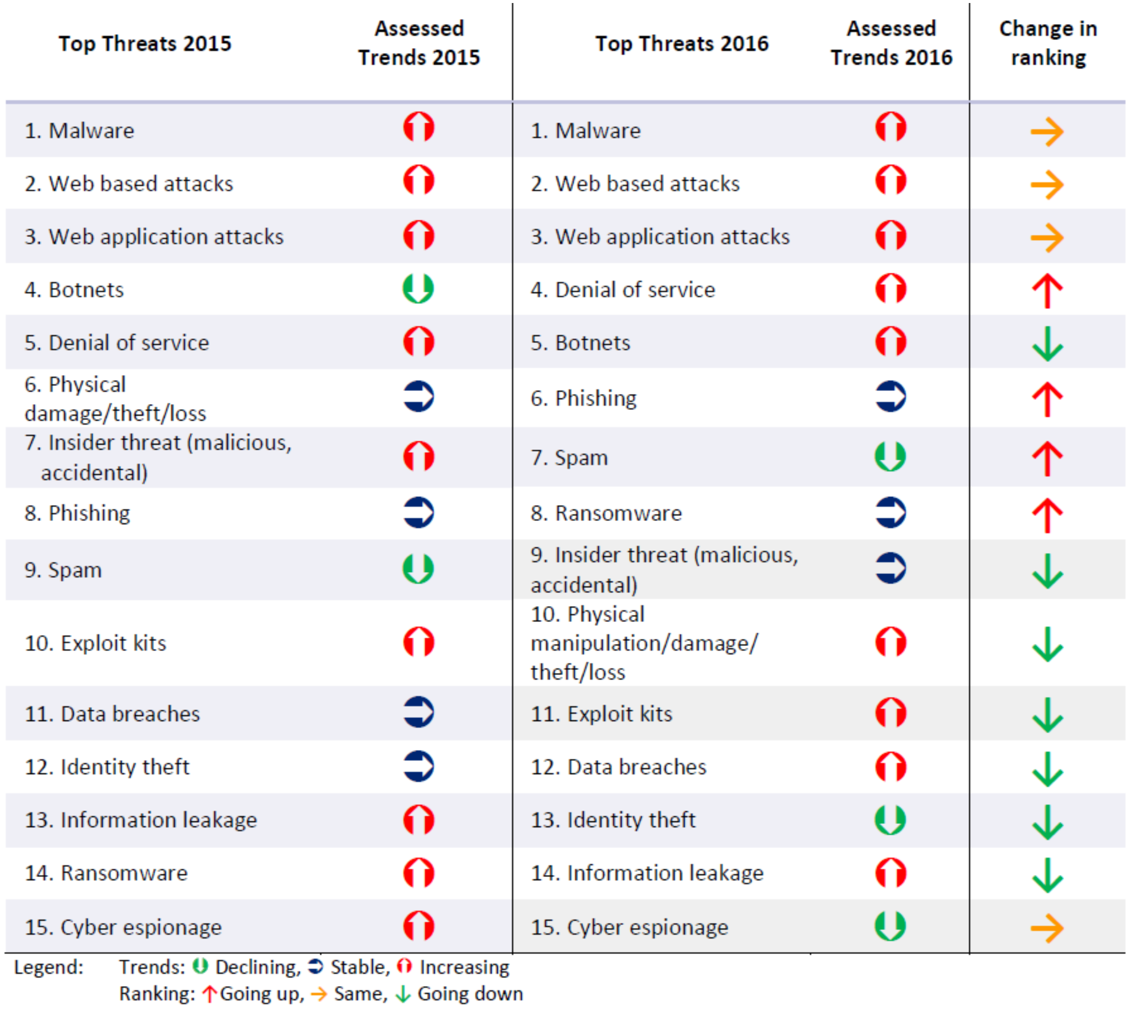
Peak into future:

- Intelligence in devices and apps
- Advanced Machine Learning
- Virtual and augmented reality
- Digital currencies and distributed ledger
- Voice based interaction with machines
- Digital labor
- Nanobot implants

*Source : KPMG study on The Creative CIO’s agenda 2016

Artificial Intelligence – our best friend or our worst enemy?

Threat Landscape



Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	⇧	1. Malware	⇧	→
2. Web based attacks	⇧	2. Web based attacks	⇧	→
3. Web application attacks	⇧	3. Web application attacks	⇧	→
4. Botnets	⇩	4. Denial of service	⇧	↑
5. Denial of service	⇧	5. Botnets	⇧	↓
6. Physical damage/theft/loss	⇨	6. Phishing	⇨	↑
7. Insider threat (malicious, accidental)	⇧	7. Spam	⇩	↑
8. Phishing	⇨	8. Ransomware	⇨	↑
9. Spam	⇩	9. Insider threat (malicious, accidental)	⇨	↓
10. Exploit kits	⇧	10. Physical manipulation/damage/ theft/loss	⇧	↓
11. Data breaches	⇨	11. Exploit kits	⇧	↓
12. Identity theft	⇨	12. Data breaches	⇧	↓
13. Information leakage	⇧	13. Identity theft	⇩	↓
14. Ransomware	⇧	14. Information leakage	⇧	↓
15. Cyber espionage	⇧	15. Cyber espionage	⇩	→

Legend: Trends: ⇩ Declining, ⇨ Stable, ⇧ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2016 with the one of 2015[1].

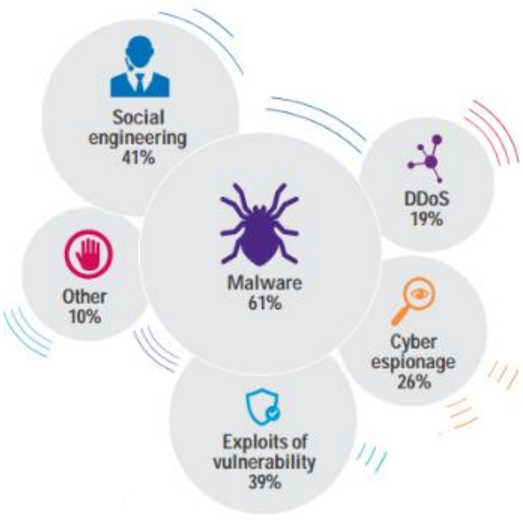
Verizon 2016 Data Breach Investigations Report 1

Information Every where…

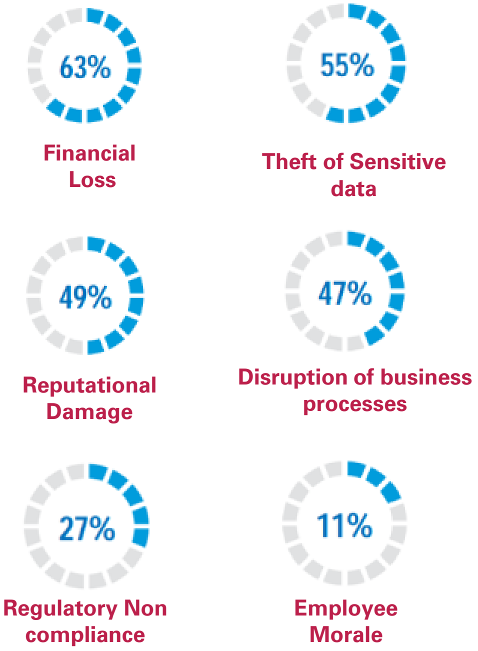
Is Security Every where?

Is traditional approach effective?

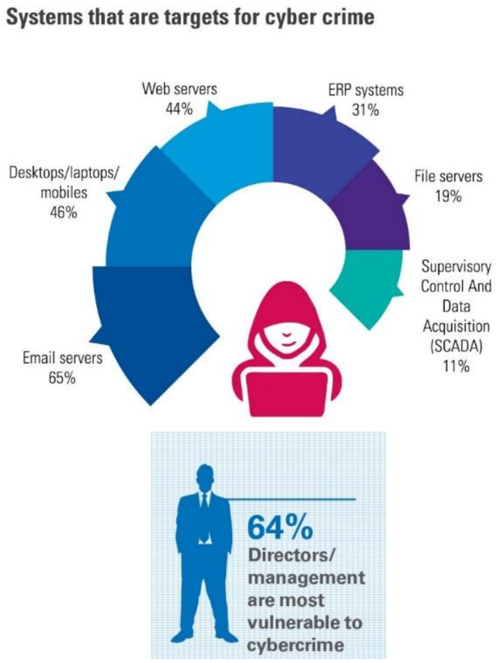
Attack vectors are changing



Cyber attacks being focused

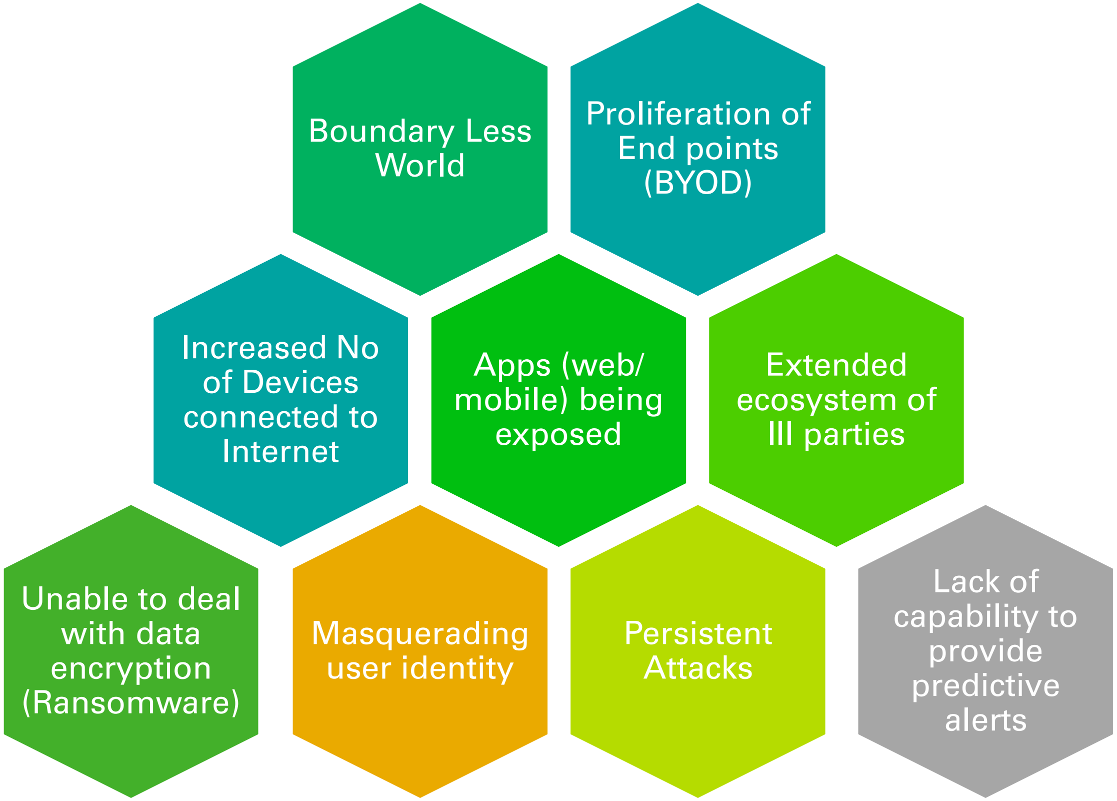


Targeted attacks



Source: KPMG Cybercrime Survey Report 2015

Limitations with traditional approach


Boundary Less World
Proliferation of End points (BYOD)
Increased No of Devices connected to Internet
Apps (web/ mobile) being exposed
Extended ecosystem of III parties
Unable to deal with data encryption (Ransomware)
Masquerading user identity
Persistent Attacks
Lack of capability to provide predictive alerts

Extra Measures

Identity Management

Third Party Risk Management

More Awareness

Proactive Identification of Changing Threat Environment

Sample Attacks - Shamoon 2.0

There are 3 components which are linked with one another which makeup Shamoon 2.0 single malware. We have analyzed each component according to the stages which the Shamoon 2.0 uses for infection on a victim's machine i.e. Dropper Component⇒ Communication Component⇒ Wiper Component.

When Shamoon 1.0 made its first wave of attack in August 2012, it had not just infected 30,000-35,000 computers but it also had crippled the entire organizations altogether which were infected with it. Its effects were seen post attack as many computers were still working irregularly and the time that required to restore the organization's full functionality led to huge loss in not just terms of money but also in terms of company’s reputation too.

The second wave Shamoon which is dubbed as Shamoon 2.0 used the similar approach which it had used previously but this time it is predicted that the amount of infection of computers will be more, since last time the attackers were able to retrieve the credentials of users for various organization, The second wave will be using the stolen credentials from the previous attack and the reason this attack is bound to be success is because of lack of awareness among the employees on securing passwords. One survey about the Middle East reports some of the facts mentioned below:

- More than 70 percent of the users said that they were storing administrative passwords in plaintext.
- Over 45 percent of the users use the same password for over multiple systems.
- More than 40 percent users share their passwords.
- Only 13 percent users change their passwords once a month.

These facts make the Middle East region more easy as a target for Shamoon 2.0

Src: http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware

OT security

Defend & Respond

Protecting Industrial Control Systems (ICS) from outside attacks can be especially troublesome when network environments allow internet access. However, it's unrealistic to operate today without the benefit of access to the Internet and to other internal systems. Therefore, the right configurations must be applied to protect this especially vulnerable area for OT systems. IT systems are typically fortified at the edge of the Internet with firewalls, proxy servers and intrusion detection services. However, within the corporate environment, sub-networks exist with much looser security barriers, due to the system and data sharing requirements between departments.

The OT environment requires a much stronger vigor to protect against attacks that might come from the Internet:

- Implement security monitoring and defensive layers to comply with standards and strengthen the security posture.
- Lower the risk of security exploits by using technical solutions, such as purpose-built industrial control security equipment.
- Set up automation and patch management tools to simplify and expedite security administration.
- Training is mandatory for operations safety, so implement the same for security.
- Train teams on what to look for and how to respond to cyber activities.

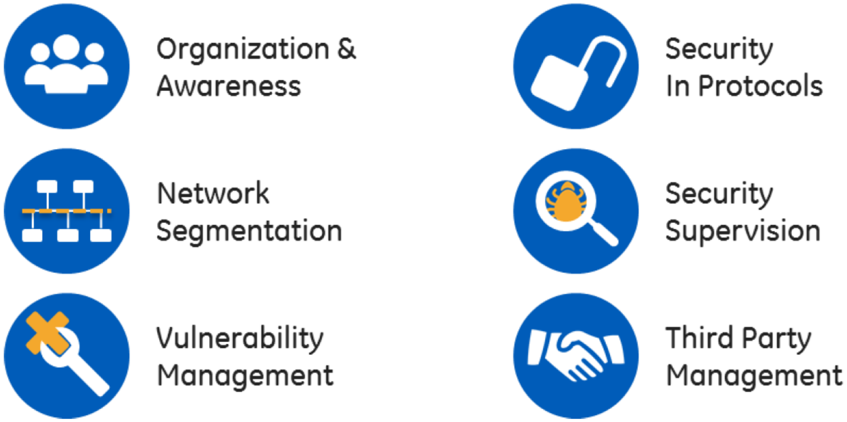
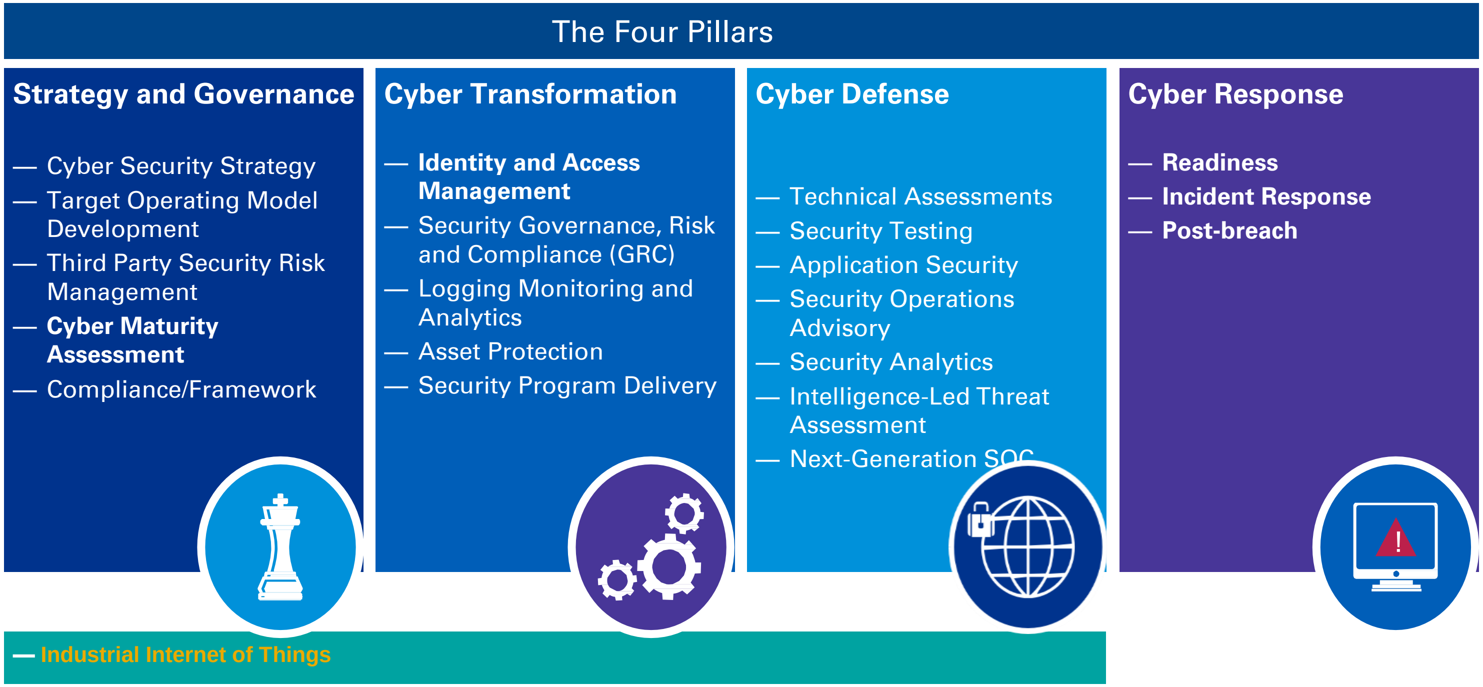


Figure 7: The areas of defense against cyber threat

KPMG Cyber Security Framework



The Four Pillars

Strategy and Governance

- Cyber Security Strategy
- Target Operating Model Development
- Third Party Security Risk Management
- **Cyber Maturity Assessment**
- Compliance/Framework

Cyber Transformation

- **Identity and Access Management**
- Security Governance, Risk and Compliance (GRC)
- Logging Monitoring and Analytics
- Asset Protection
- Security Program Delivery

Cyber Defense

- Technical Assessments
- Security Testing
- Application Security
- Security Operations Advisory
- Security Analytics
- Intelligence-Led Threat Assessment
- Next-Generation SOC

Cyber Response

- **Readiness**
- **Incident Response**
- **Post-breach**

— **Industrial Internet of Things**

And Measures to Combat Cyber Threats are Evolving...

Thank you

KPMG

Download on the App Store

kpmg.com/socialmedia

kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.