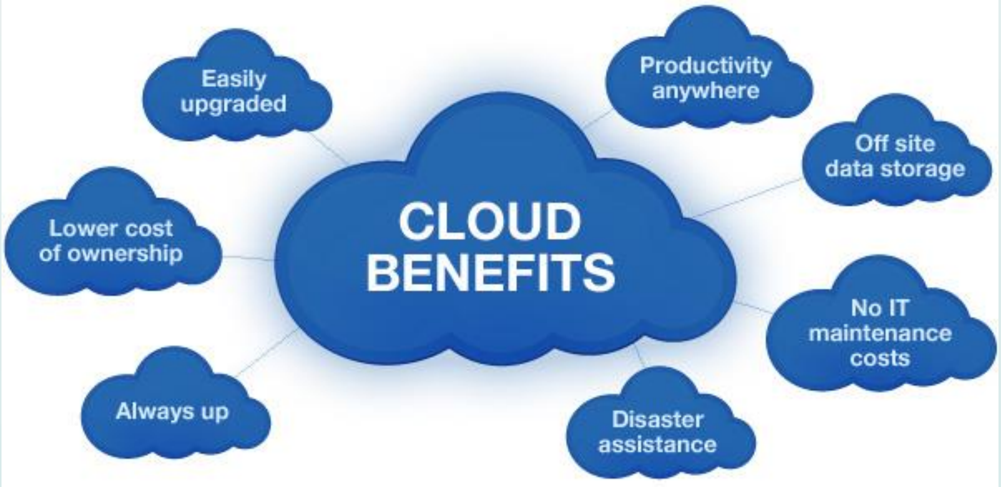
9 WORST CLOUD SECURITY THREATS

Costas Tritsaris
IT Operations Officer EMEA - Wirecard NZ Limited
Marketing Director - ISACA Athens Chapter

CLOUD TECHNOLOGY



Fresh Software

Do more with less

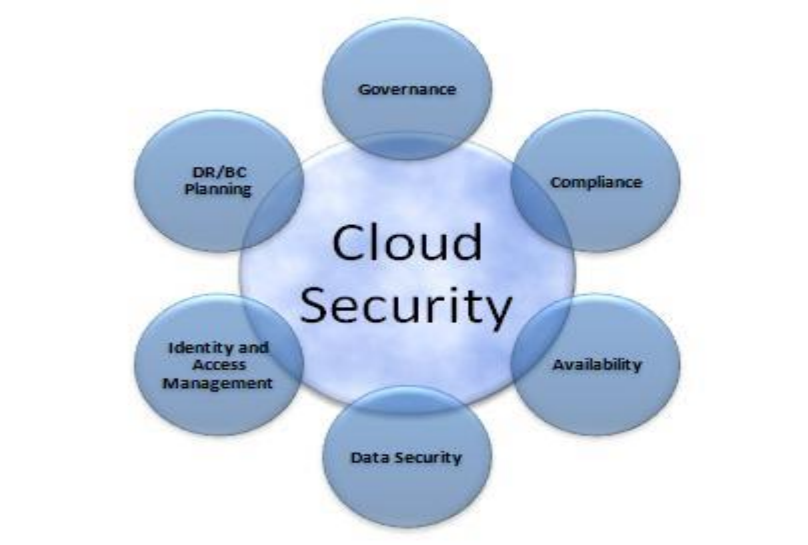
Flexible costs

Always on availability

Improved mobility

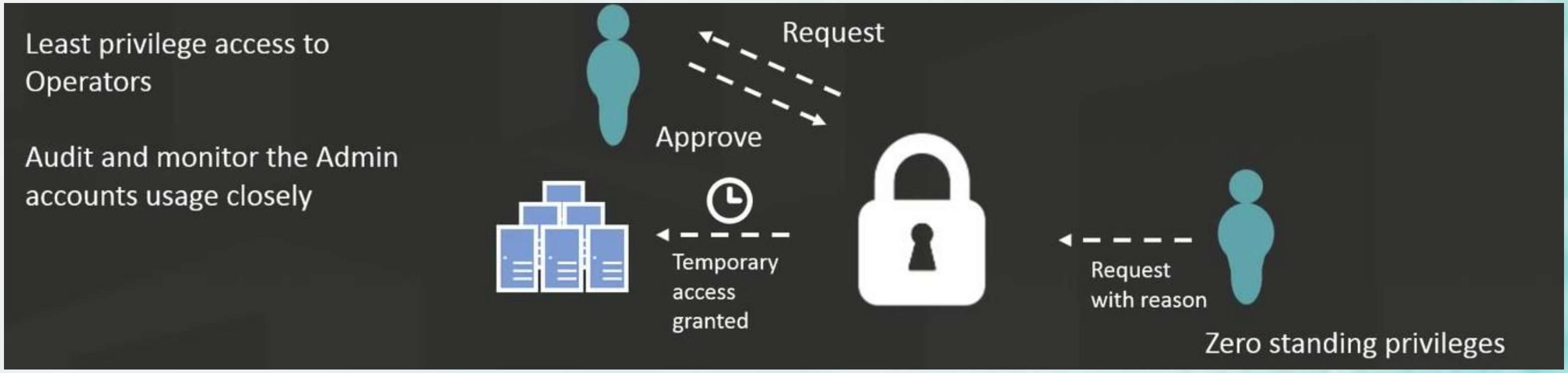
Flexible capacity

CLOUD SECURITY



What about security threats in cloud environments?

MALICIOUS INSIDERS



Least privilege access to Operators

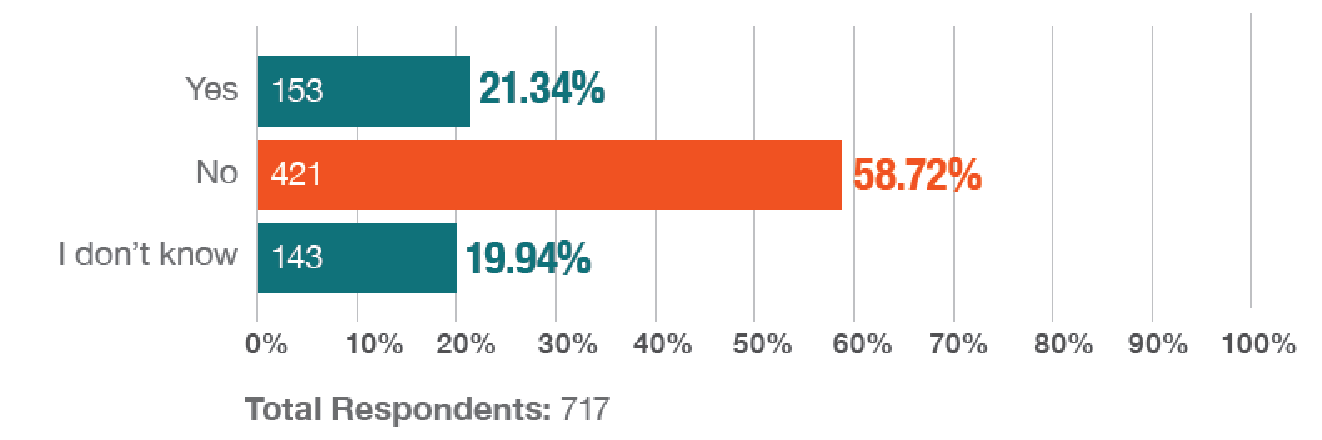
Audit and monitor the Admin accounts usage closely

- ❑ keep encryption keys on cloud customer’s premises, not in the cloud
- ❑ Just in time elevations with zero standing permissions
- ❑ Clear auditing and logging of all Lockbox actions
- ❑ Automation tools to run all regular tasks
- ❑ New comers Background checks
- ❑ control the encryption process and keys, segregating duties and minimizing access given to users

MALICIOUS INSIDERS

Enterprises Victimized by Cybercrime

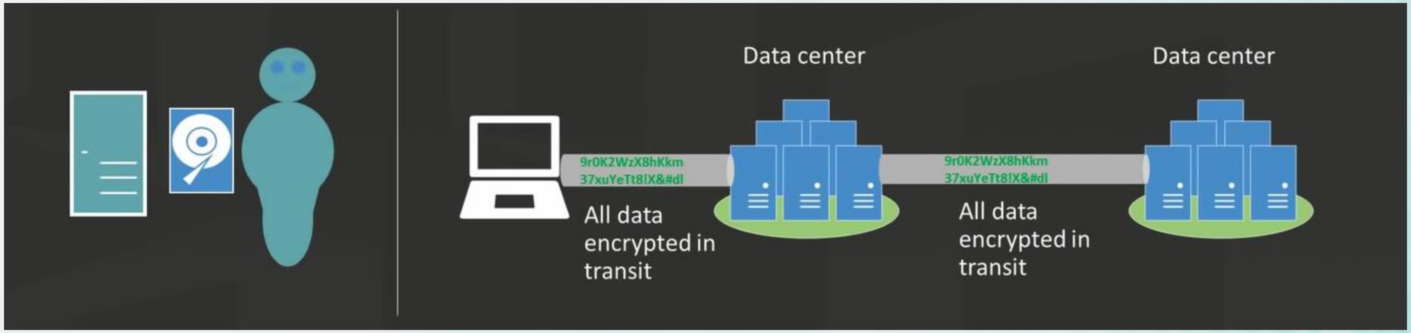
Question: Has your organization been part of a cybercrime during 2014?



A deeper dive into the enterprise cybercrimes reported by 21% of respondents reveals that 82% of the crimes were identified by an internal source.

Source: ISACA and RSA Conference Survey

DATA BREACHES



Media breach

- ❑ Physical Security
- ❑ Laptop and Desktop lockers.
- ❑ Encryption at all.

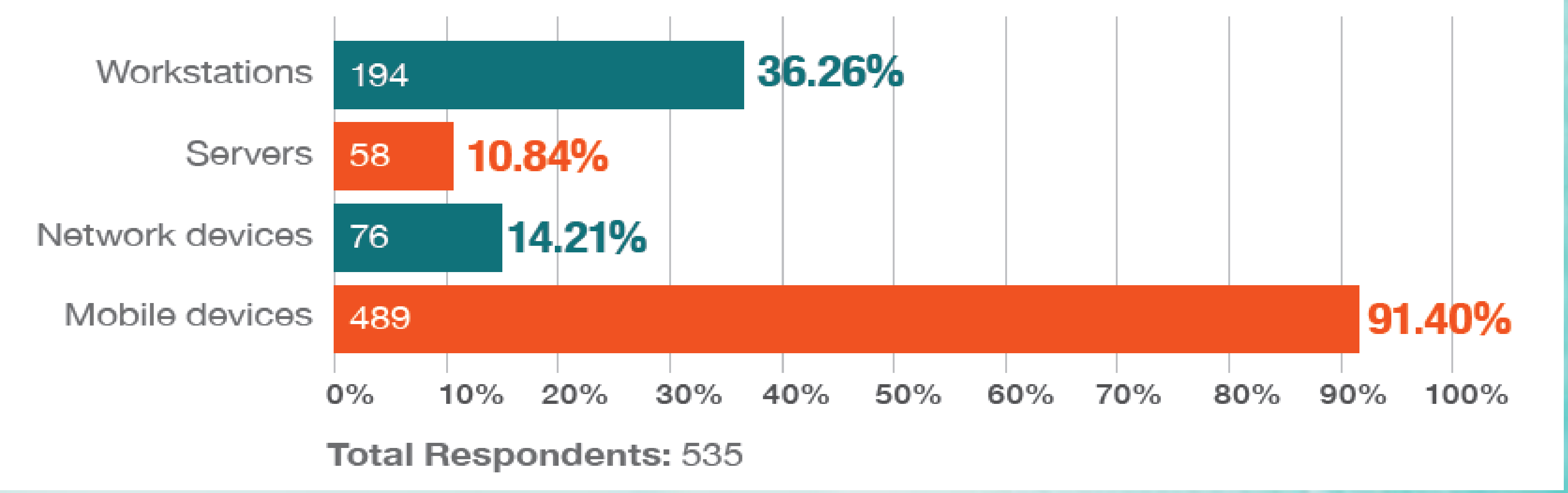
Man in the Middle

- ❑ Encryption in transit within and outside datacenters
- ❑ End-to-end encryption using S/MIME , PGP
- ❑ Message encryption using RMS, OME

DATA BREACHES

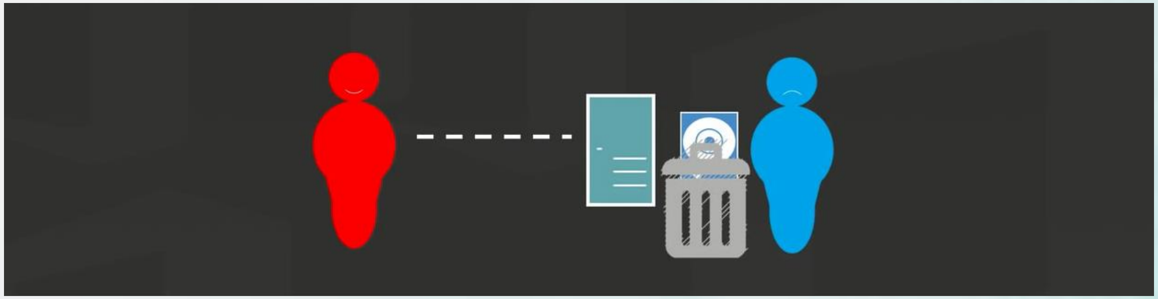
Lost Physical Devices

Question: Has your organization experienced physical loss of assets in 2014? What type of assets?



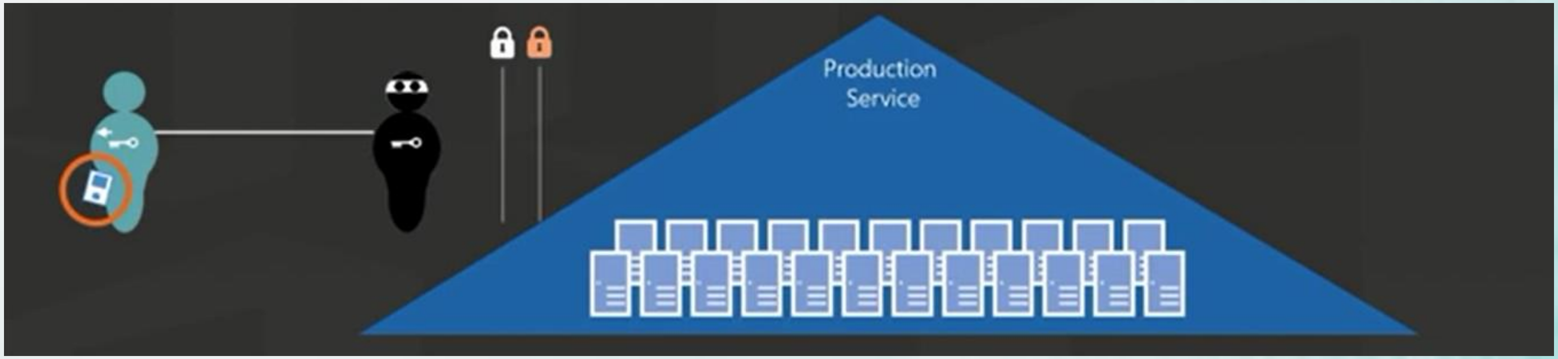
Source: ISACA and RSA Conference Survey

DATA LOSS



- ❑ Archive / Backup versioning
- ❑ Users/Admin level – recycle bin
- ❑ Can get data for period of time.
- ❑ Redundancy for natural disasters (Data replication)
- ❑ Disk Mirroring
- ❑ Ineffective or non-existence of CP
- ❑ Have a plan that works, to mitigate the attack before it occurs (Cyberattck).

ACCOUNT OR SERVICE TRAFFIC HIJACKING

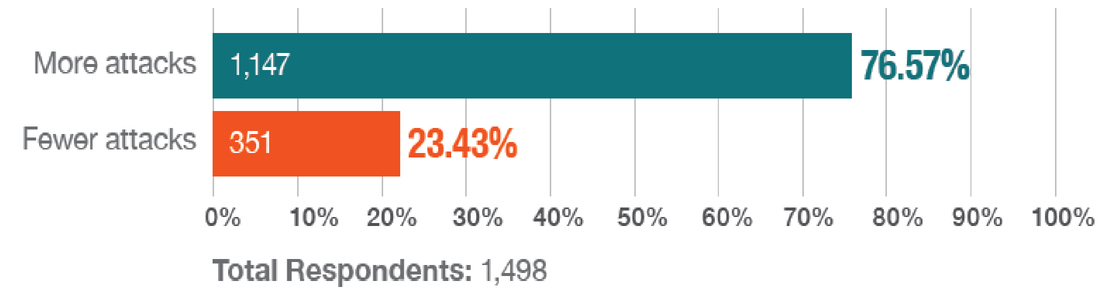


- ❑ Multi-factor authentication
- ❑ Strong password policy
- ❑ RBAC within the tenant
- ❑ Limited admin accounts
- ❑ Social Engineering (Reduce the risk from Phishing Attacks, Baiting Scenarios, Quid Pro Quo, Piggybacking, Creating distrust and other cyberattacks)

ACCOUNT OR SERVICE TRAFFIC HIJACKING

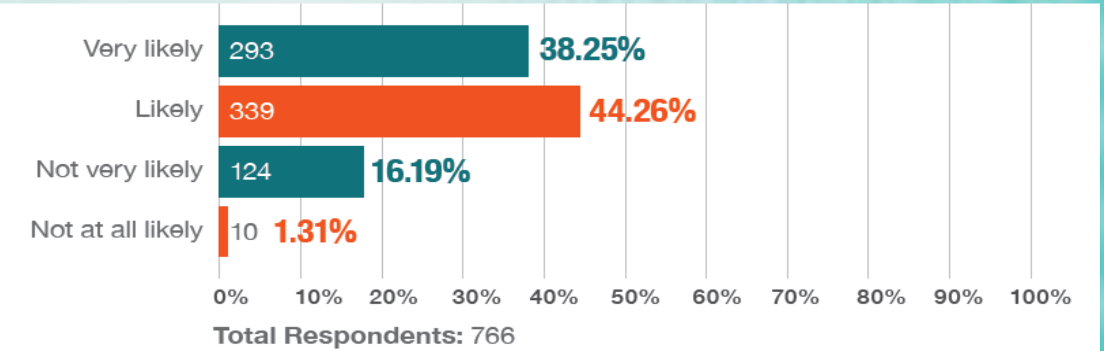
Number of Cyberattacks in Respondents' in 2014 vs 2013

Question: In 2014 has your enterprise experienced an increased or decreased in security attacks as compared to 2013?



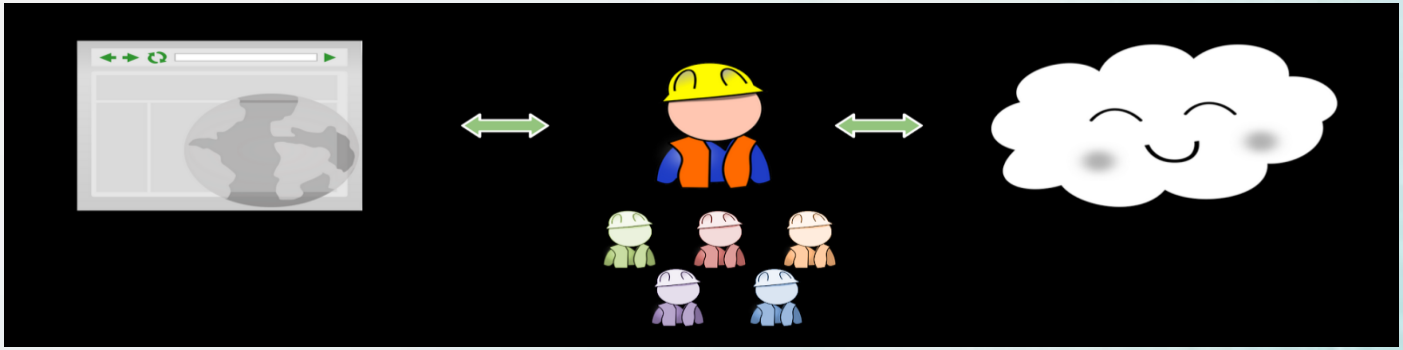
Likelihood of Cyberattacks in Respondents' Enterprises in 2015

Question: How likely do you think it is that your organization will experience a cyberattack in 2015?



Source: ISACA and RSA Conference Survey

INSECURE APIS



□ Authentication

□ Access control

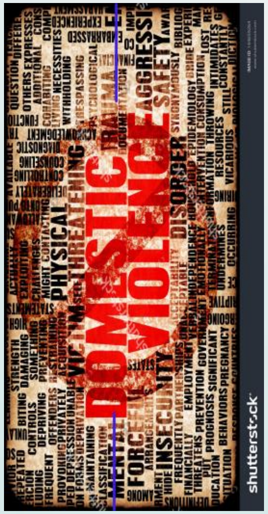
□ Encryption

□ Activity monitoring

□ Penetration testing

□ Have a plan that works, to mitigate the attack before it occurs (Cyberattck).

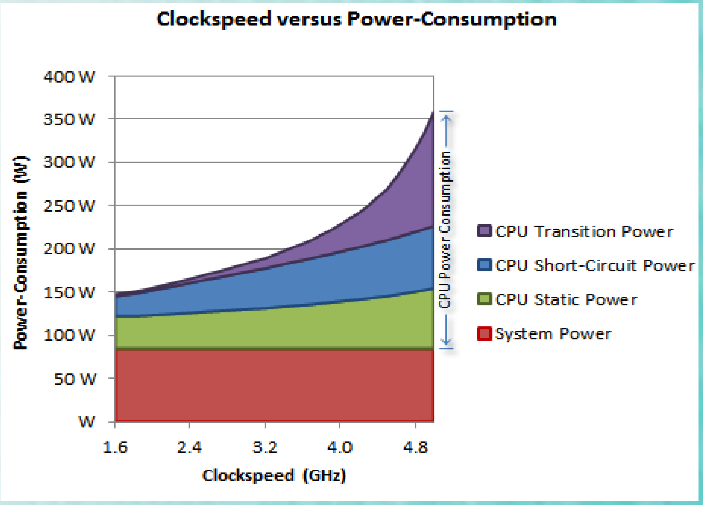
ABUSE OF CLOUD SERVICES



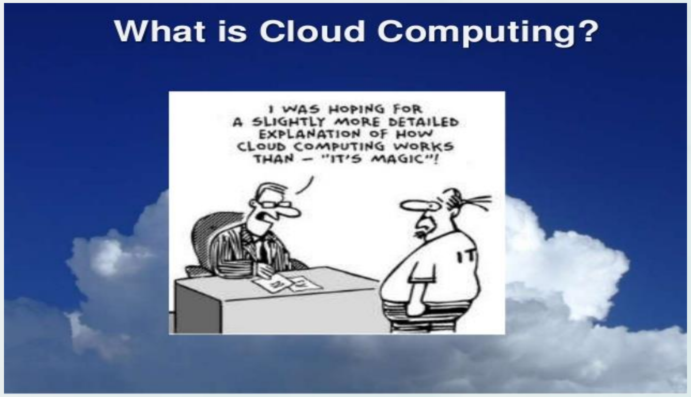
- It might take an attacker years to crack an encryption key using his own limited hardware. But using an array of cloud servers, he might be able to crack it in minutes
- Lack of abuse detection allows cloud instances to be used like botnets
- Poor or Lack of capacity planning

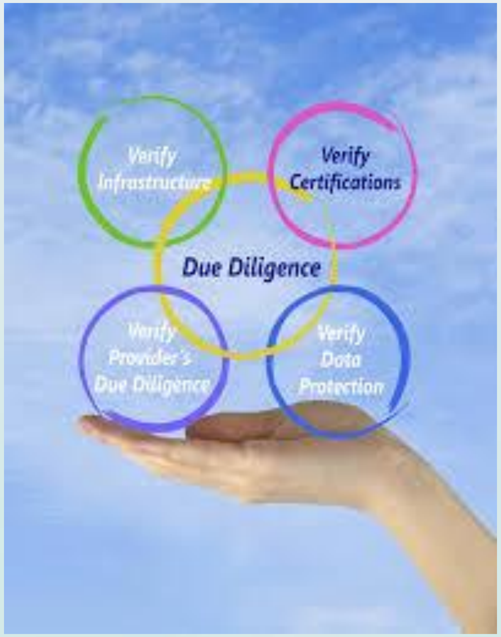
DENIAL OF SERVICE

- Denial of service attacks are an old disrupter of online operations, but they remain a threat
- For cloud customers, experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock
- Because of its complexity, it’s recommended to have a team of experts to provide guidance as to the best preventive measures to mitigate threats.
- Have a plan that works, to mitigate the attack before it occurs (Cyberattck).



INSUFFICIENT DUE DILIGENCE


What is Cloud Computing?
I WAS HOPING FOR A SLIGHTLY MORE DETAILED EXPLANATION OF HOW CLOUD COMPUTING WORKS THAN – "IT'S MAGIC"!
IT



❑ Understanding of the service providers' environment and protections

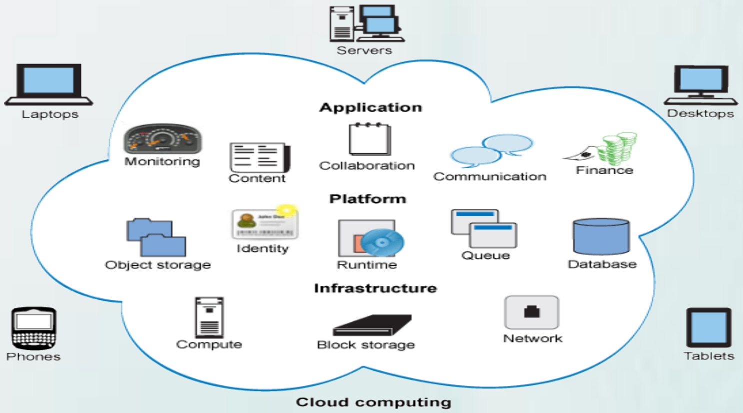
❑ enterprises must always remember to involve the IT team before introducing any cloud computing initiatives to the organization

❑ take the necessary measures to ensure that the IT infrastructure of an enterprise remains secure from any cyber attacks

❑ How will liability be divided?

❑ How much transparency can a customer expect from the provider in case of an incident?

SHARED TECHNOLOGY – SHARED DANGERS

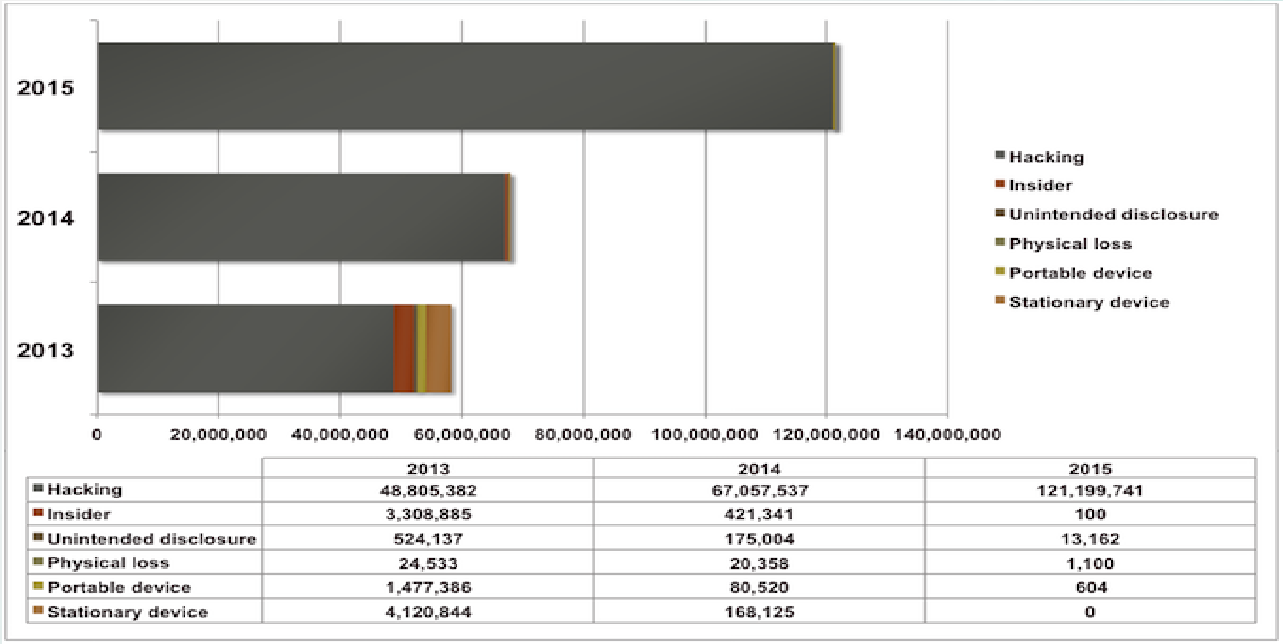


- ❑ In a multi-tenant environment, the compromise of a single component it exposes the entire environment to a potential of compromise and breach.

- ❑ a misconfigured operating system or application can lead to compromises beyond their immediate surroundings

- ❑ Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects everyone.

OBSERVATION OF CLOUD VULNERABILITY INCIDENTS DATA BREACHES STATISTICS 2015



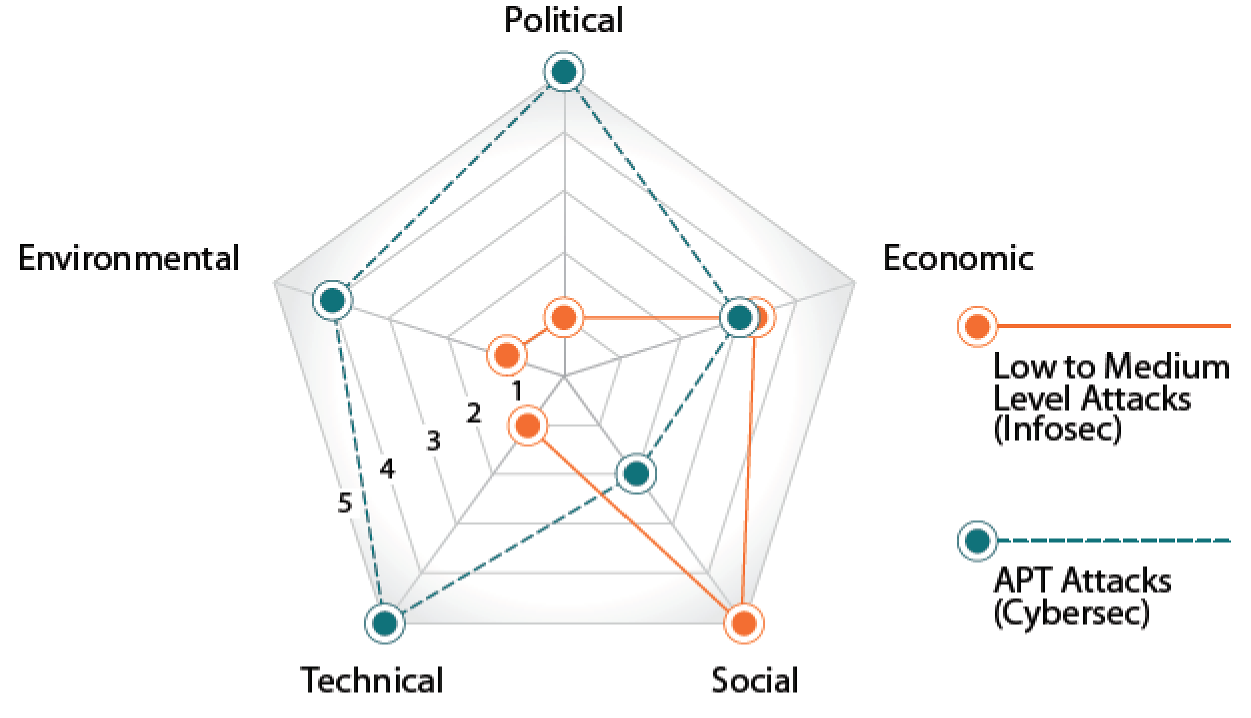
	2013	2014	2015
Hacking	48,805,382	67,057,537	121,199,741
Insider	3,308,885	421,341	100
Unintended disclosure	524,137	175,004	13,162
Physical loss	24,533	20,358	1,100
Portable device	1,477,386	80,520	604
Stationary device	4,120,844	168,125	0

External hacking	99% in 2015 and growing
Insider attacks	decreasing
Physical loss	decreasing
Portable device	decreasing

Source : SecurityWeek.com / August 2015

INFORMATION SECURITY AND CYBERSECURITY FOCUS (PESTLE)

The difference between the areas covered by cybersecurity and the areas covers by traditional information security.



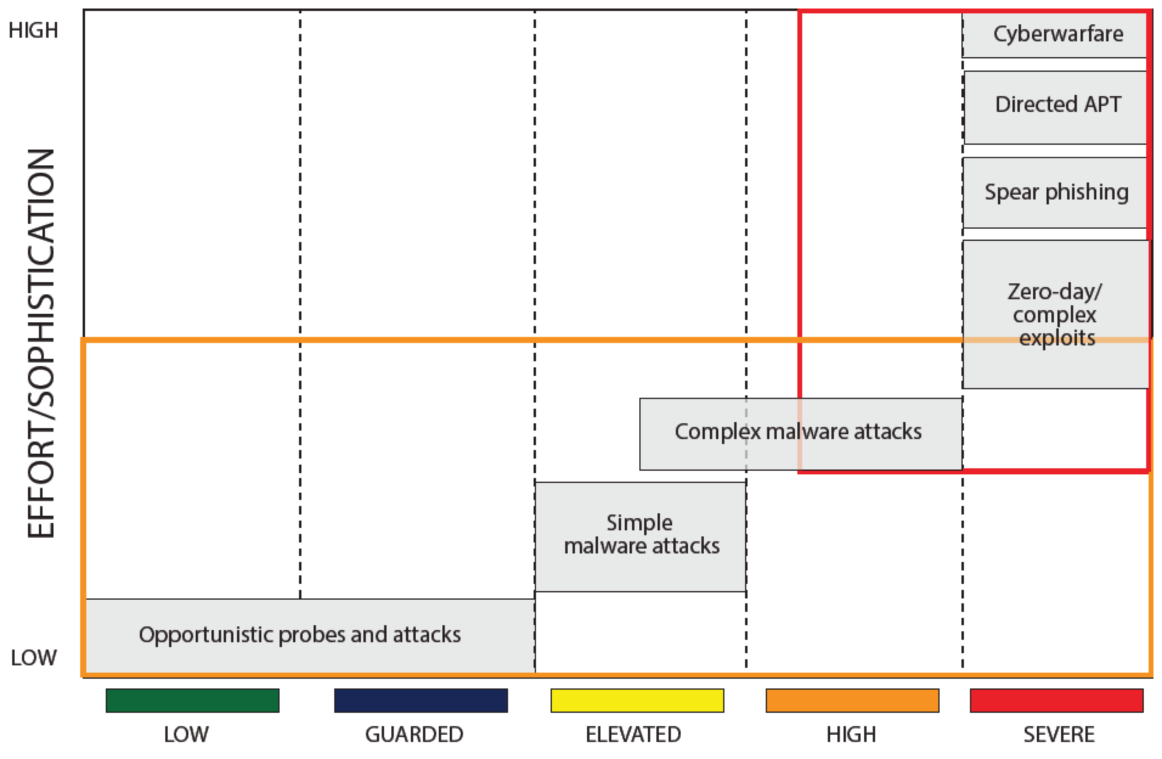
Source: ISACA and RSA Conference Survey

ATTACKS AND THREAT LEVELS

Threat levels and the types of cyberattacks, based on their required effort and sophistication. The red rectangle denotes the type of attacks and threat level usually covered by cybersecurity and the remaining area is covered by information security.

🟥 Cybersecurity scope

🟧 Information security scope



Source: ISACA and RSA Conference Survey

CYBERSECURITY NEXUS

2015 GLOBAL CYBERSECURITY STATUS REPORT

Global survey of more than 3,400 ISACA members in 129 countries

86% of respondents see a global cybersecurity skills gap

92% of them are planning to hire more cybersecurity professionals

83% of respondents say cyberattacks are among the top three threats facing organizations

38% say they are prepared to experience one

Cybersecurity is a global issue—and it’s everyone’s responsibility

Cybersecurity (CSX) Certifications

❑ CYBERSECURITY FUNDEMENTALS CERTIFICATE

For college students, recent graduates, those new to cyber security, as well as those looking to change careers. Provides the basic theoretical knowledge for Cybersecurity, including key concepts and terminology as well as basic guidance to build fundamental cybersecurity controls.

❑ CSX PRACTITIONER

An entry-level certification for professionals who want to demonstrate technical skills and abilities in cyber security. Certifies hands-on experience which enables candidates to be a first responder to cyber incidents, following established procedures and defined processes.

❑ CSX SPECIALIST

For professionals who want to demonstrate deeper intermediate technical skill in a specialty area within cyber security. Each of the five certifications, certifies effective skills and deep knowledge in the respective five areas Identify, Detect, Protect, Respond and Recover, aligned to the NIST Cybersecurity Framework.

General overview for Greece

- ❑ CSX was introduced in 2015.
- ❑ Great demand for security-related skills, also in the Greek job market. GR Firms have been actively hiring security professionals at both technical and managerial levels in the past years.
- ❑ CSX Fundamentals is an entry-level certification.

ISACA Athens Chapter – CSX - Training

- ❑ Organizes Cybersecurity Fundamentals training twice a year.
- ❑ Has organized two CSX Fundamentals training with great success.

Cybersecurity
Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

7½ MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *2014 Internet Security Threat Report, Volume 19,* Symantec, April 2014; **2.** *M-Trends 2014: Attack the Security Gap,* Mandiant, April 2014; **3.** *Increased Cyber Security Can Save Global Economy Trillions,* McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study,* ISACA, April 2014; **5.** *An Executive's Guide to 2013 Data Breach Trends,* Risk Based Security/Open Security Foundation, February 2014; **6.** *ISACA's 2014 APT Study,* ISACA, April 2014; **7.** *ISACA's 2014 APT Study,* ISACA, April 2014; **8.** *Code.org,* February 2014; **9.** *2014 Cisco Annual Security Report,* Cisco, January 2014; **10.** *Cybersecurity Skills Haves and Have Nots,* ESG, March 2014

CSX CYBERSECURITY NEXUS

ISACA®
Trust in, and value from, information systems

MAY 2014

CYBERSECURITY NEXUS

THANK YOU

Trust in, and value from, information systems