# Someone will click that link…
## and it is not always so obvious

**Nice to Know You**

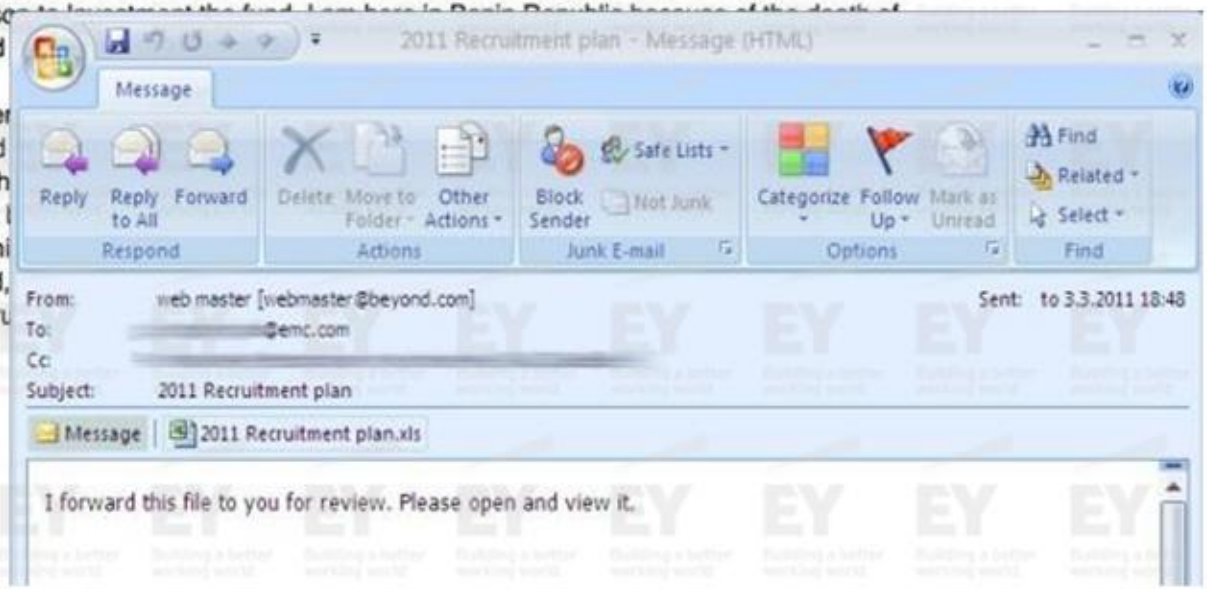
• Naomi Surugaba [azlin@moa.gov.my]

Inbox

Actions

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy perso
my parent`s and
purpose.
Please I will offer
transfer the fund
country due to th
medical student
email:missnaomi
Remain blessed,
Miss Naomi Suru




**23%** of users will OPEN phishing emails

**11%** will CLICK on attachments

Source: Verizon Data Breach Investigations Report 2015

# Someone will click that link…
## and it is not always so obvious

**LESSON LEARNED:**

Cybersecurity awareness for end-users

# Security exploitation is an Industry

Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim

Cybersecurity firm has 400GB of what purport to be its own documents published via its Twitter feed after hack

Hacker For Hire Professional Services | Hire a Hacker Online
centralhacker.com/
Professional **Hacker** for hire Online! Email or password **hacking** facebook **hacking**, web h
and more! Hire a **hacker** today!

Hire a hacker, hacker for hire, hire professional hacker, hire hackers
**hacker**1337.com/
hire a **hacker** online that is professional! Email password **hacking**, facebook **hacker**, web
**hack** university and many hackers for hire **services**.
Services Payment Method Password Cracking Email Hacking

Golden Group | Hacking Services
https://www.goldengroup.org/en/**hacking-services**/index.php
Golden Group is a group of hackers that offer a lot of **hacking services** for a cheap price. With us, you can get any password from any account, or fake hacking

Email hacking services
https://**hackemails**.biz/
We offer your our help in professional **hack** of email passwords!

# Security exploitation is an Industry

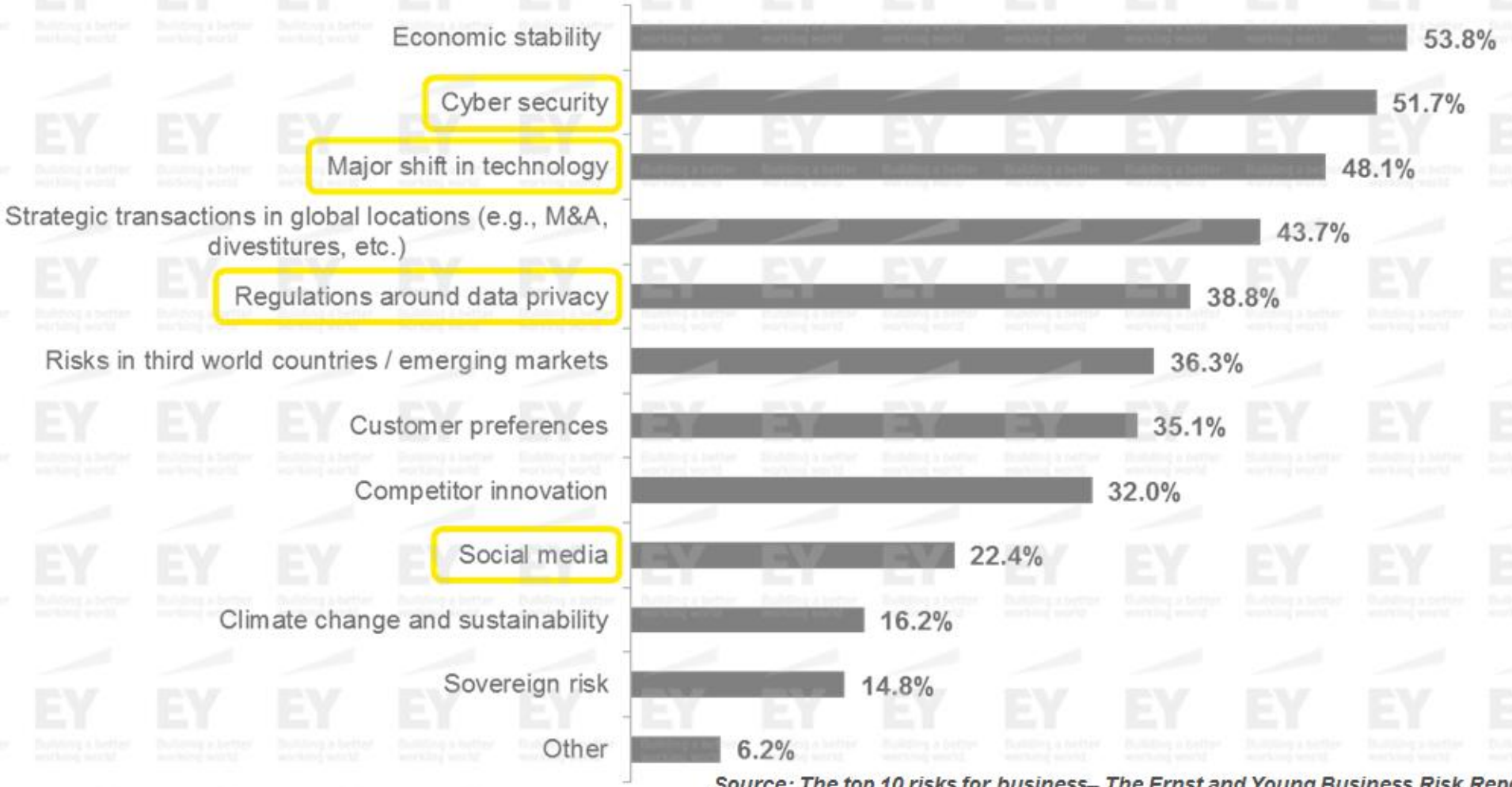
**LESSON LEARNED:**

Cybercrimes now are **HIGHLY ORGANIZED, HIGHLY FOCUSED** and **HIGHLY SKILLED** organization

# IT related risks gain in Importance

*4 of the Top 10 Emerging Risks are IT related*

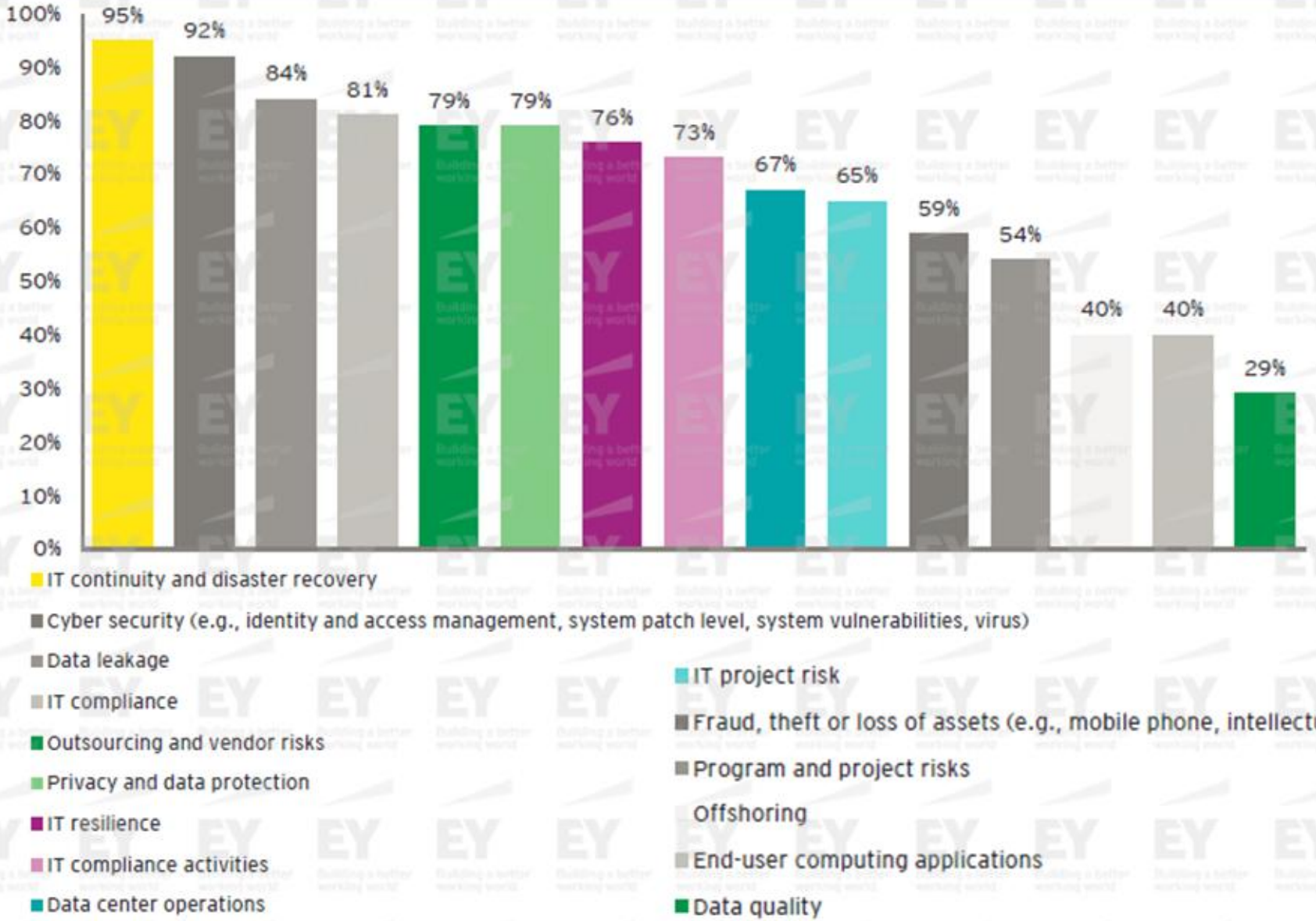
## The most significant emerging risks according to Chief Audit Executives (CAEs):




***Source: The top 10 risks for business– The Ernst and Young Business Risk Report***

# Top risks managed by IT Risk Management function

*Top the risk list are IT continuity, Cyber security and Data leakage*




***Source: Ernst and Young IT Risk Management Survey***

# Technology Gaps & Risks

1980s

Computer virus
Phone phishing
Dumpster diving

1990s

Mail spam, mail phishing
Web phishing
Keylogger

2000s

Mobile virus
Spyware, adware, trojan
Automated toolkit

2010s

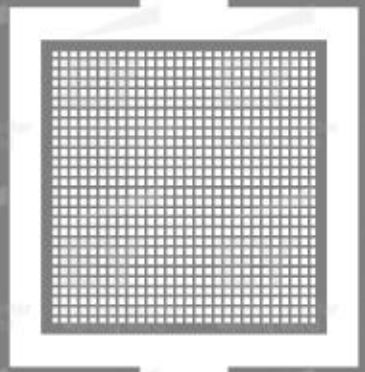
Instant messenger spam
Ransomware
Social engineering

2020s

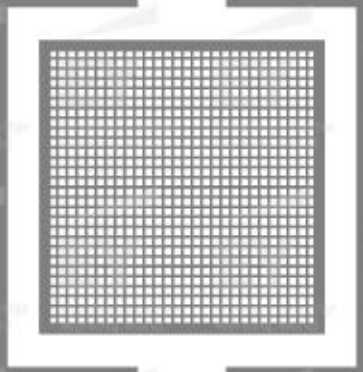
???

**2.** If you're under cyber-attack, would you ever know?

**- Live demo**



# 3. How to defend? What is the approach for security practices?



# IT and Cyber Security, what are the challenges?

Building a better working world

# Resources Constraints Challenges

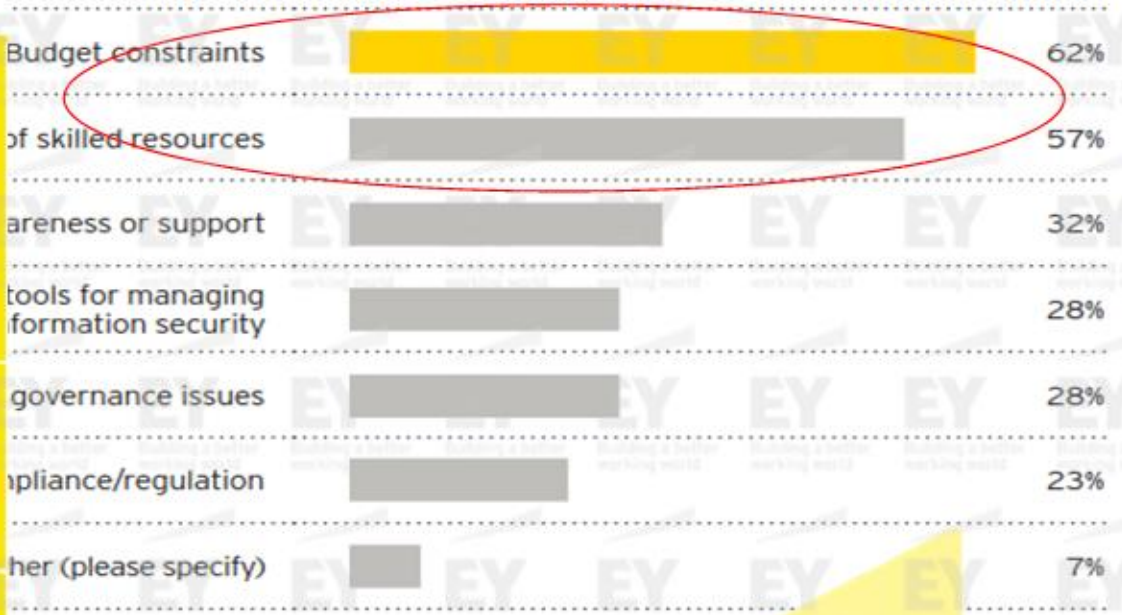
**57%** of respondents — **LACK OF SKILLED RESOURCES** is challenging information security's contribution and value to their organization

**88%** of organizations — their information security is **NOT FULLY MEETING THEIR NEEDS**

**54%** of organizations — **DO NOT currently have a role or department in their information security function** that is focusing on emerging technology and its impact

**47%** of respondents — **DO NOT** have a **Security Operations Center**

Key challenges to organizations' information security



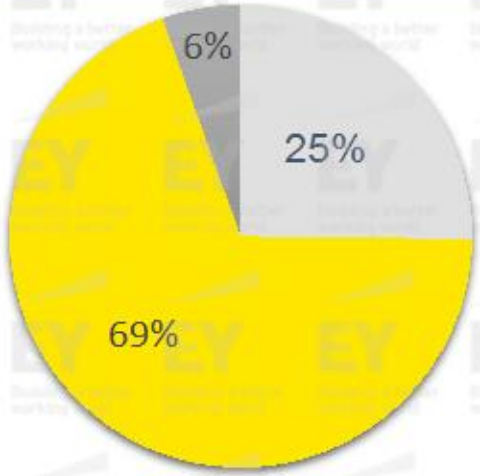

**60%** respondents — do not believe their staff can handle anything beyond simple cybersecurity incidents

**68%** respondents — do not consider monitoring their business ecosystems as an information security challenge

Sources: EY's Global Information Security Survey 2015
An ISACA and RSA Conference Survey 2016

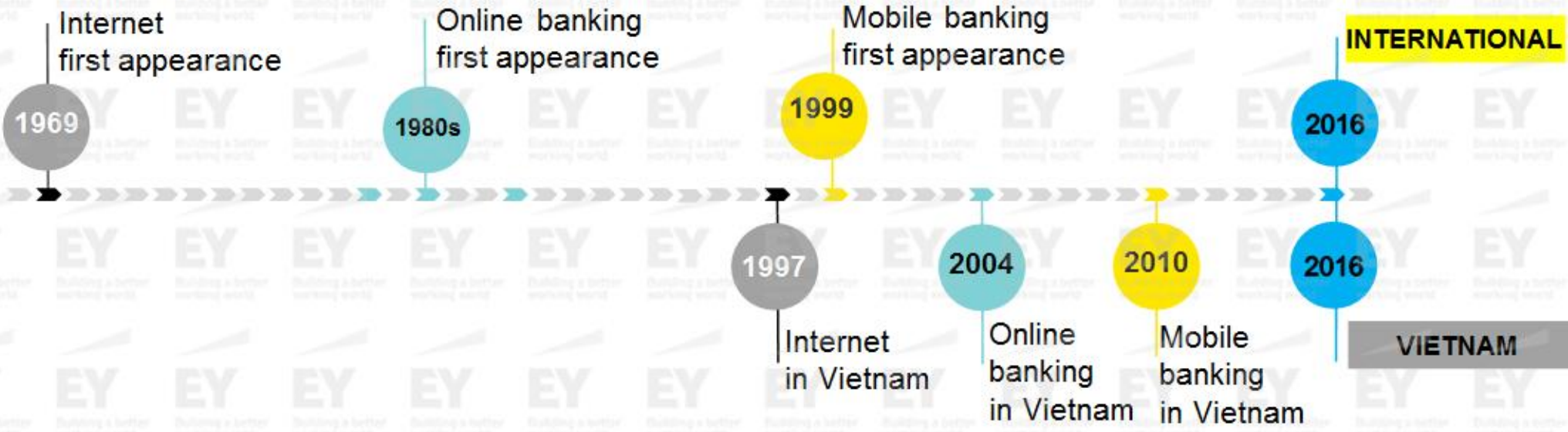
# In Vietnam: Young Population & Technology fast evolution

## Young people




- percentage of population under 15
- percentage of population between 15 and 64 years old
- percentage of population 65+

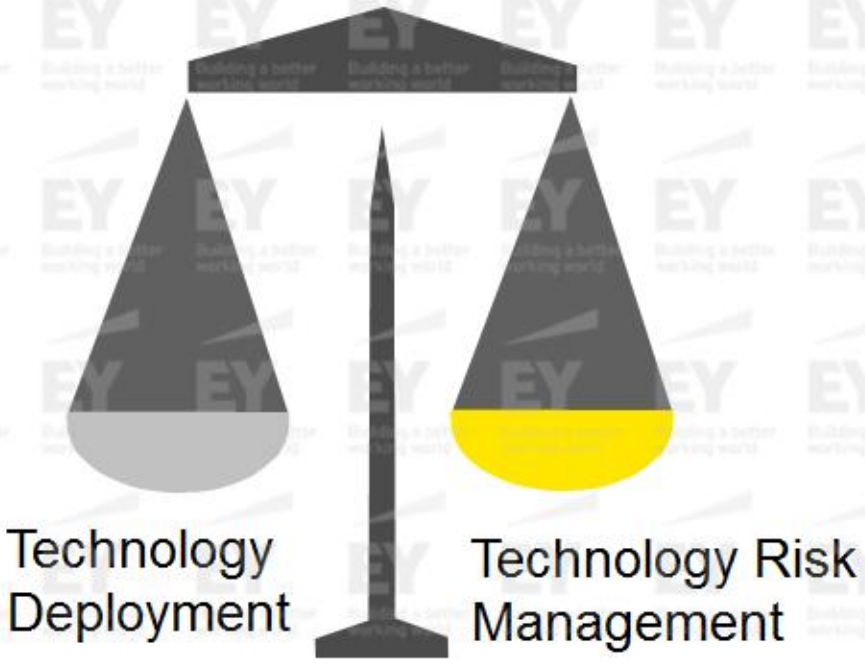
## Technology Gap



# What is the approach for security practices?

Building a better working world

# Balance between Technology Deployment and Technology Risk Management



# You can't avoid being attacked or breached

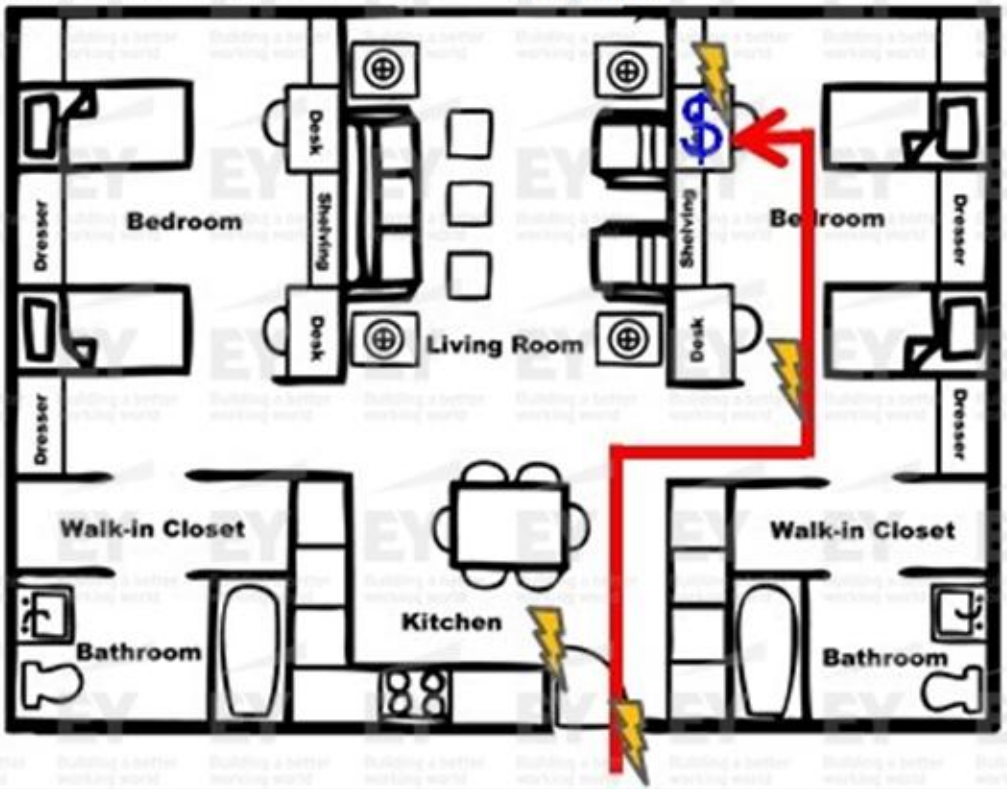
*Let's think how to protect your dollars in your house…*

To protect our house, where should we implement our protection?

- Alarm at main door?
- Camera?
- Bedroom door?
- Safe box?

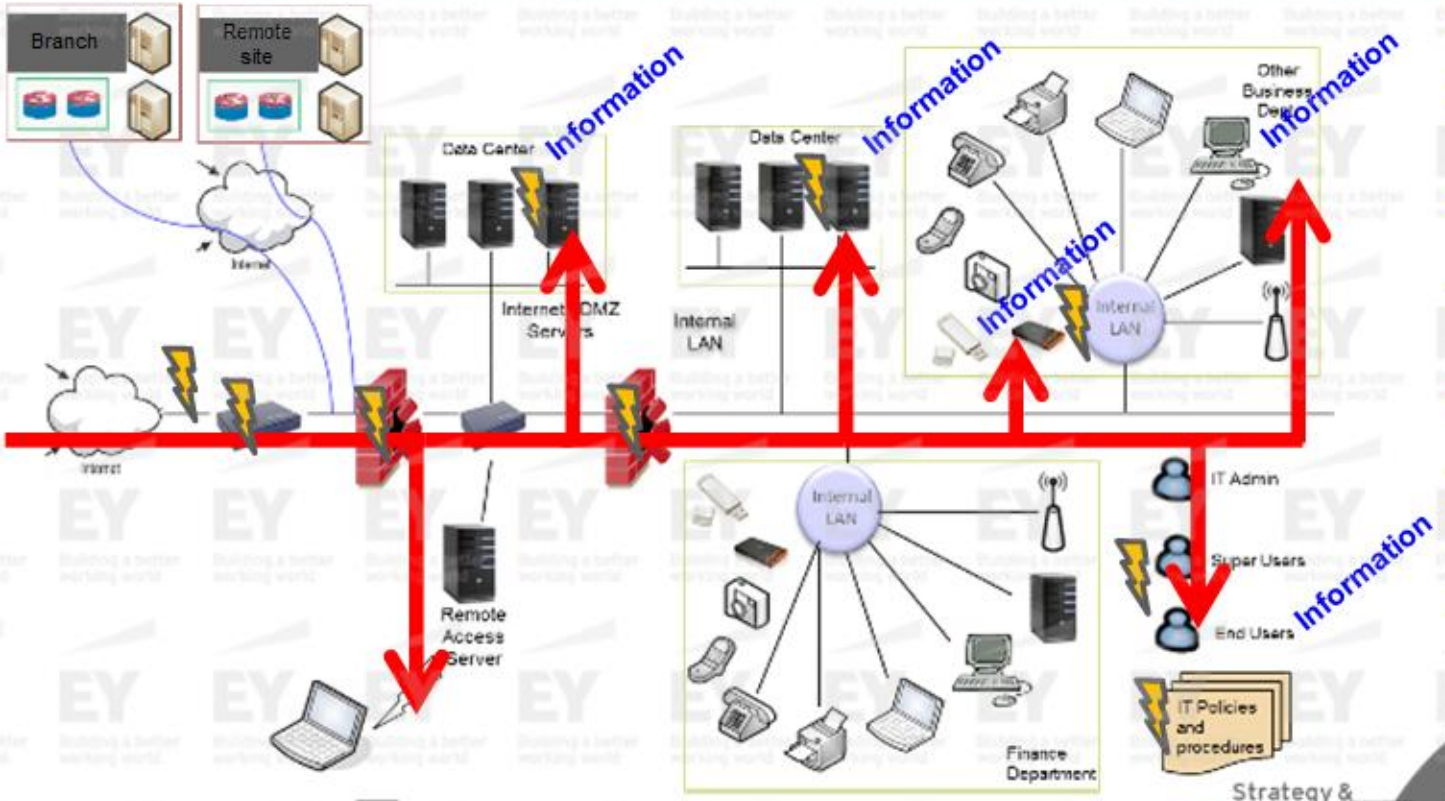
- Ask yourself, are those protections sufficient and adequate?
- What are other possible threats?

- Fence?
- Front gate?
- Garage door?
- Windows?
- Roofs?
- Chimney?
- Back doors?

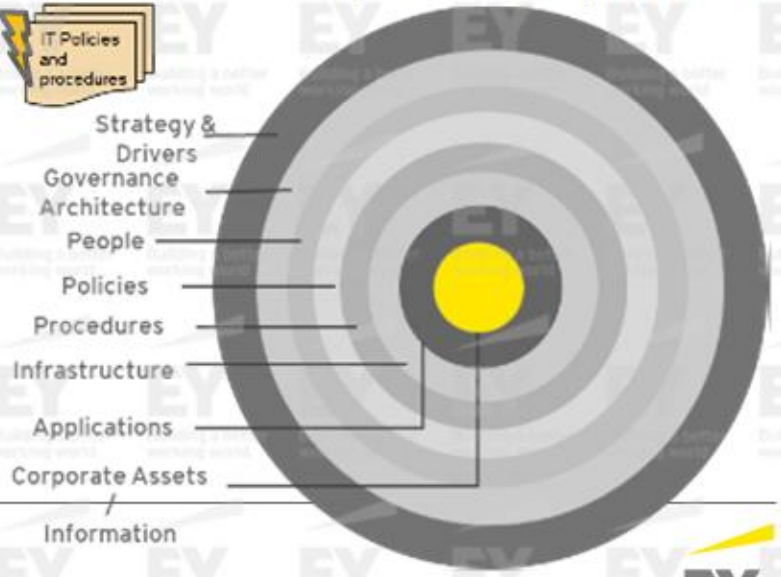


# You can't avoid being attacked or breached

*…and now how to protect your Corporate Information*




- Physical security (building, offices…)
- Router security settings
- Firewall security settings
- Server security settings
- Lan network design and security settings
- HR scanning; Awareness training
- Information security policies and practices




- There are "**layers of security defense**" that a corporate can implement to protect their **selected valuable information**

# How to start Cybersecurity Management?

The starting point for gaining confidence is to understand what you look like to a cyber attacker.

1. How can you **protect** your organisation if you do not know what it is the attackers are targeting?
2. How will they **gain access** and how would this damage you and your critical assets?
3. Do you fully **understand** your organisation's ability to respond, contain and recover from an attack?

**Approach**

Applying **Risk Management** to **Cyber risk management** is a useful way to think about cybersecurity

# The 3 lines of defence (LOD)

**1st Line of Defence**

Management designing, implementing and operating core business operations and support functions, such as IT Finance, HR, etc.

**2nd Line of Defence**

Monitoring, assessing the design of risks and controls for their efficiency and effectiveness. Advise on the design of the controls and processes.

**3rd Line of Defence**

The third line of defence consists of objective, independent control evaluation and monitoring functions – usually performed by internal audit or contractors.

# Risk Management Life-cycle

**Process**

"IT Risk Universe"

"Information Asset"

"IT Environment"

**"Product"**

1. IT Risk Management Methodology and Governance
2. IT Risk assessment framework
3. Technical Risk Assessment methods/technique
4. Risk assessment plan (periodically/ randomly)
5. IT audit plan (periodically/ randomly)
6. Various risk assessment reports

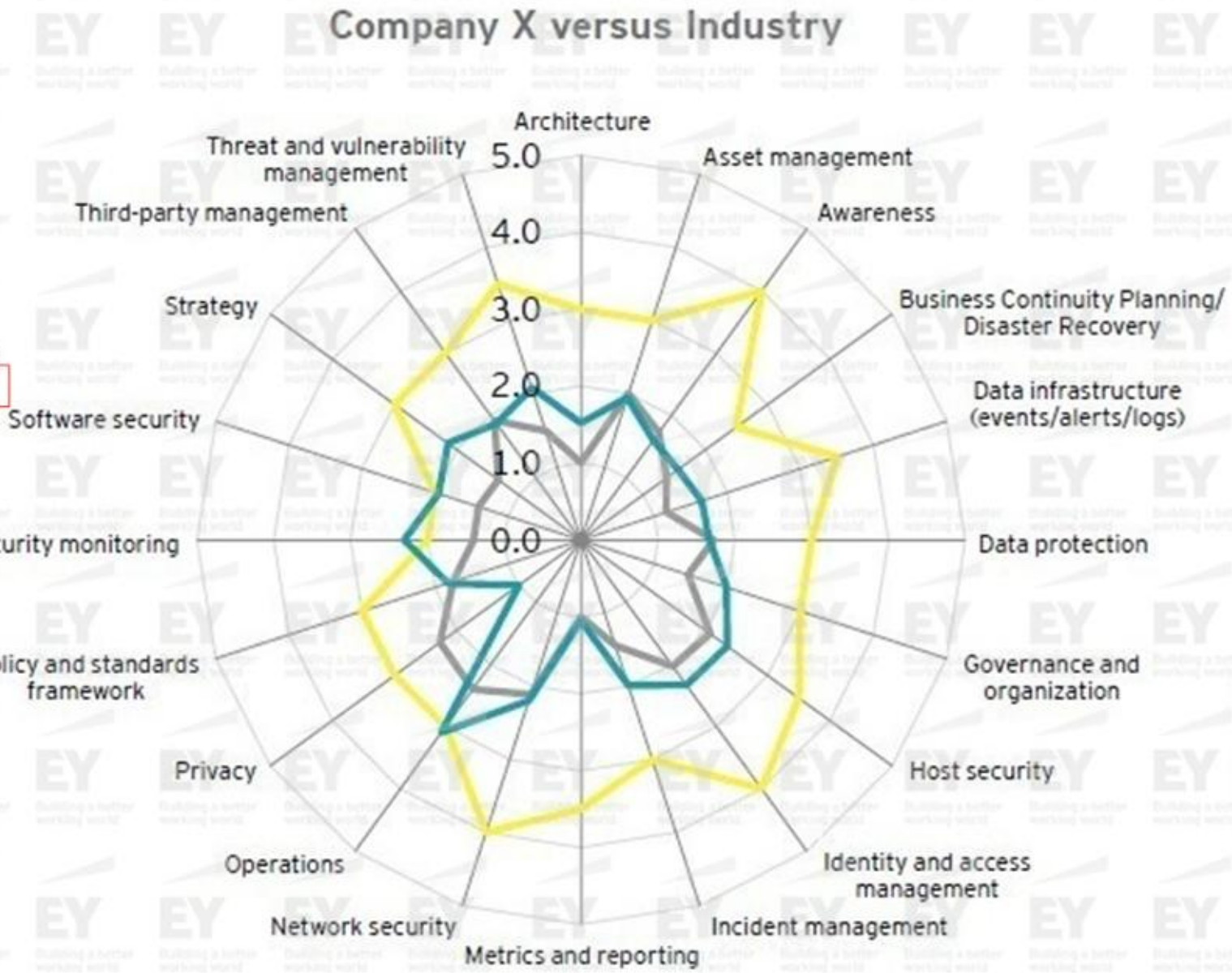
# Conduct Cybersecurity Health check



32%

of respondents stated that benchmarking information about the maturity of peer organizations was the most useful and their highest priority

## Cyber Program Management - EY's current state maturity benchmarking tool



# Technical Vulnerability Assessment and System Penetration Testing

## Scope:

- Website
- Mobile Application
- Infrastructure
- Wireless …

## Types:

- Back/ Grey/ White box
- External
- Internal

## When:

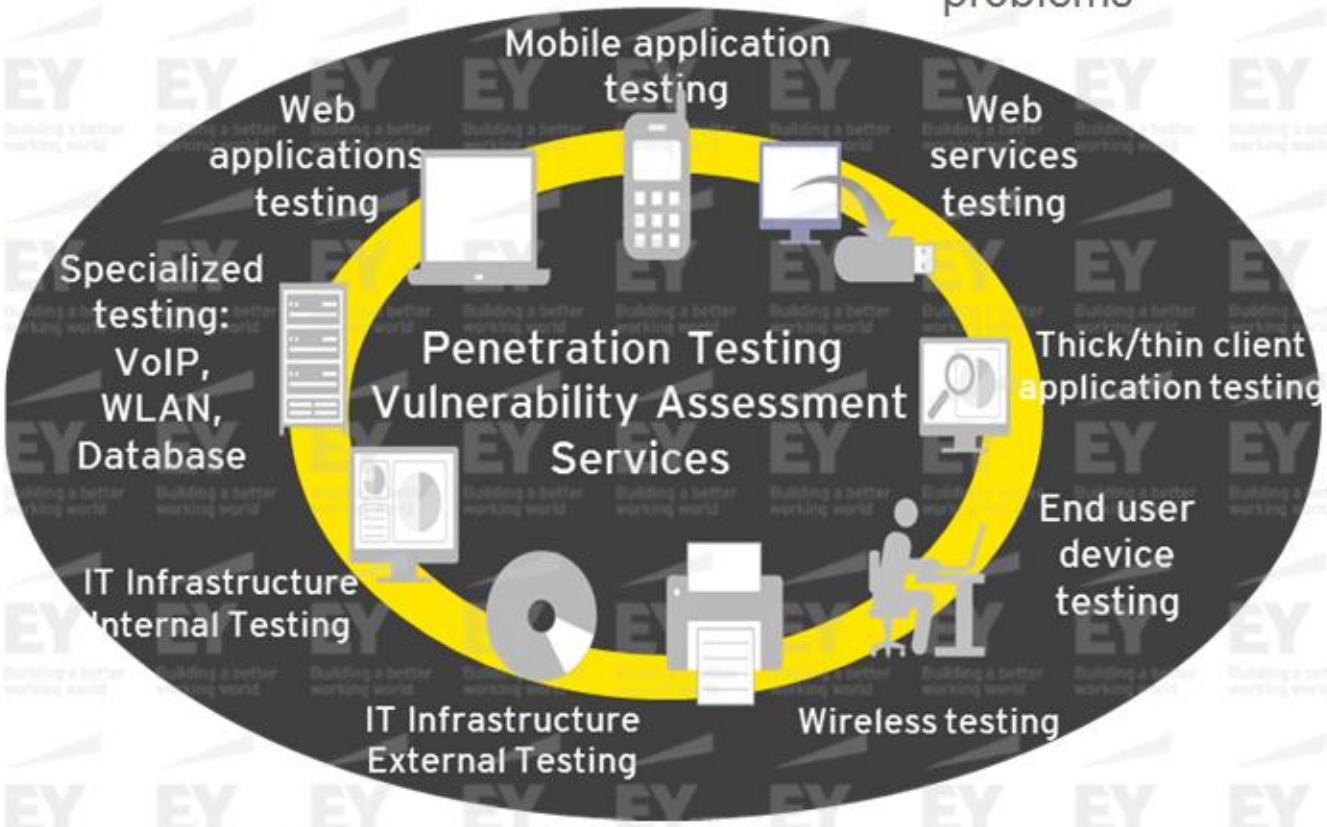
- Periodical review/testing
- Before system go-live
- Before update patch/upgrade
- …

## Objectives may include:

- Identification of vulnerabilities
- Testing the testers' skills
- Testing response/defenses

## Caution:

Fixing all your vulnerabilities does not solve your security problems




Discovery → Vulnerability identification → Exploitation → Reporting

Typical VA/PT Approach

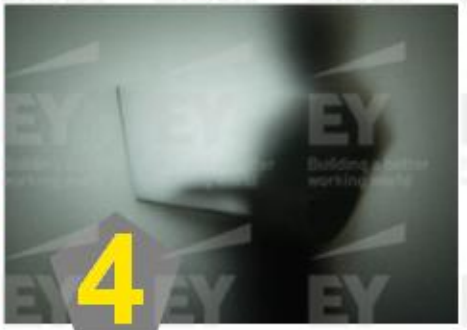
# Security Configuration Management/ Baselines

**Security hardening**: locking down systems to their most secure configurations and not running services that are not required

**Objective:** Configuring systems to be 'as secure as possible'

**Sources of baselines for security hardening**:

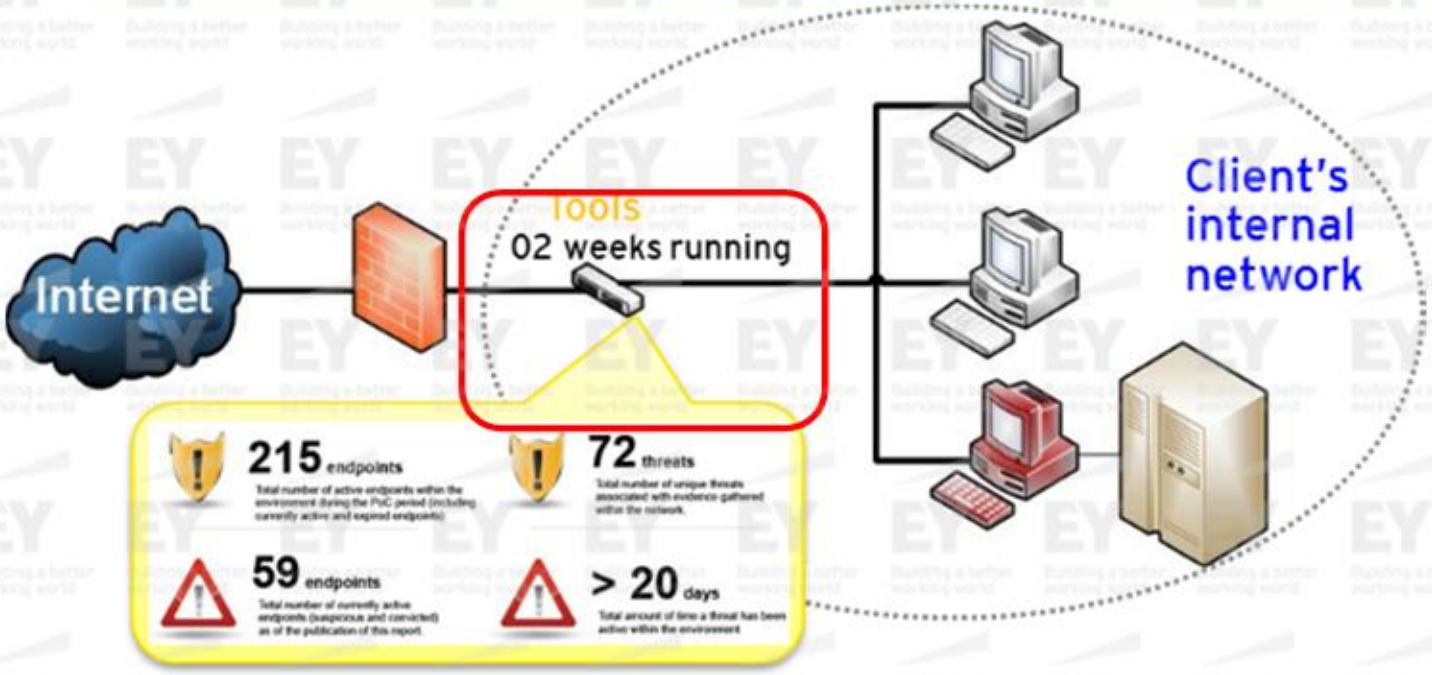
- Vendor guidance (e.g. *Microsoft, Oracle, SAP*, etc.)
- Security industry groups (e.g. *CIS, NIST, SANS*, etc.)




**Common issues and concerns**:

- Application compatibility
- Policy exceptions and tracking
- 'Softening' over time

# Cyber Compromise Assessment
## *"Indicators of Compromise"*




**Internal network traffic analysis**

- Unauthorized access of servers
- Automated activities such as OS updates, email retrieval or instant messaging alerts

**Cybercrime intel**

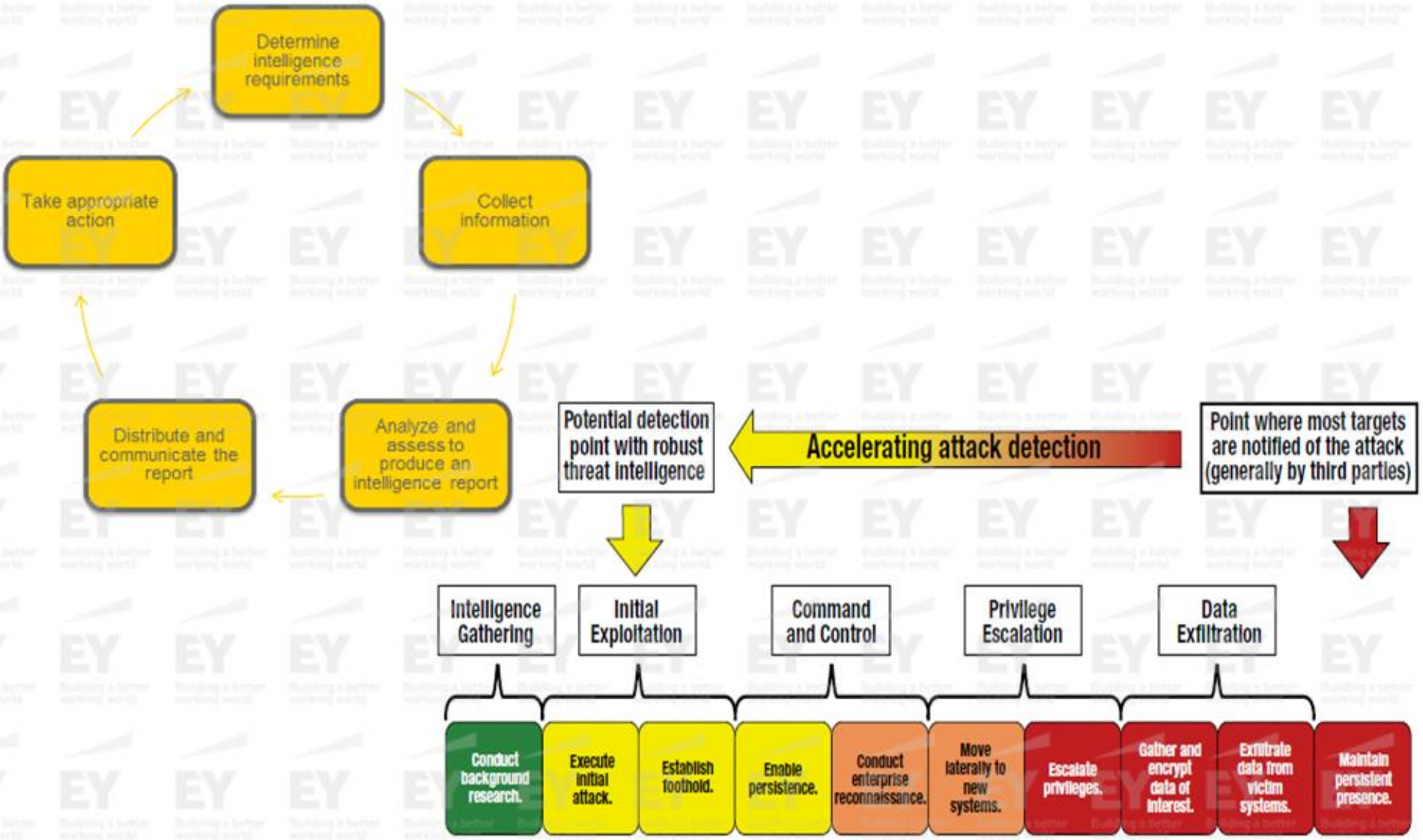
- Raw data relevant to the organization
- Employee data such as userIDs, password
- Open source feeds and underground feeds
- Blacklist host feeds

**Are you Compromised ?**

**External communication analysis**

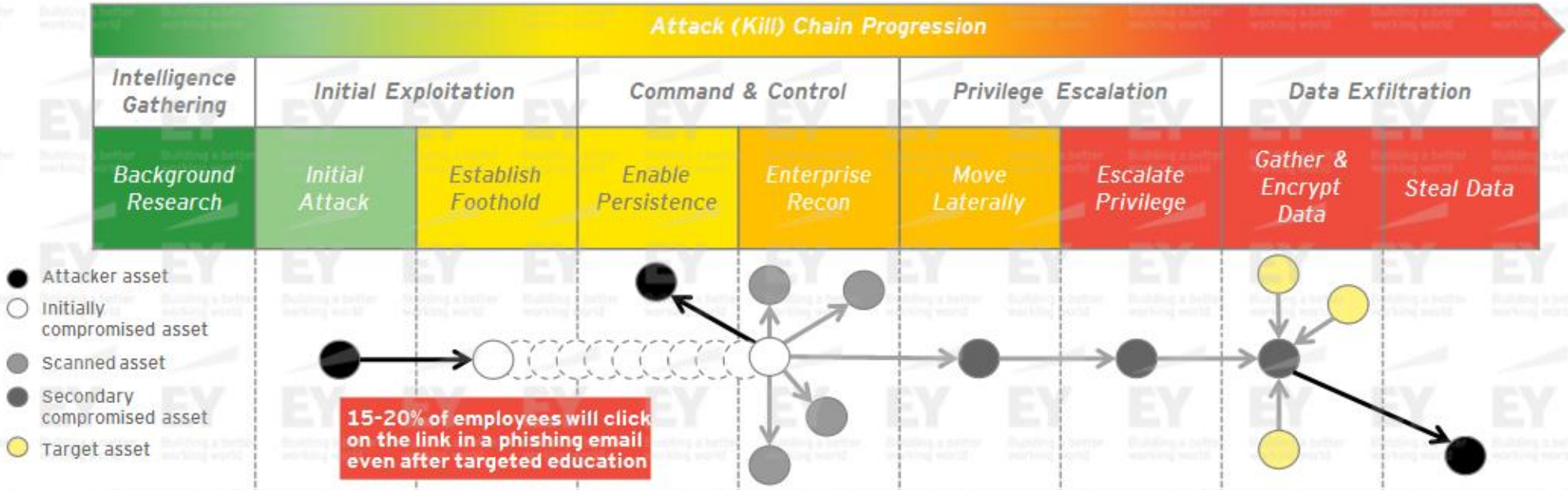
- C&C activities such as data exfiltration
- Incoming DOS attacks
- Sending of unknown messages to C&C servers at standard timings

# Threat Intelligence



# Alignment of Detection Capabilities

## *Applying NextGen Cyber Analytics to a typical Attack Chain*




| Data Sources | Intelligence Gathering | Initial Exploitation | | Command & Control | | Privilege Escalation | | Data Exfiltration | |
|---|---|---|---|---|---|---|---|---|---|
| | Background Research | Initial Attack | Establish Foothold | Enable Persistence | Enterprise Recon | Move Laterally | Escalate Privilege | Gather & Encrypt Data | Steal Data |
| | ► Social media<br>► Email logs<br>► Proxy logs (email)<br>► Proxy logs (web)<br>► ePO agents | ► Proxy logs (web)<br>► Proxy logs (email)<br>► Email logs<br>► ePO agents<br>► AD logs<br>► AV logs | ► ePO agents<br>► AD logs | ► ePO agents<br>► DNS<br>► AD logs<br>► AV logs | ► ePO agents<br>► DNS<br>► NetFlow | ► AD logs<br>► DNS<br>► NetFlow | ► AD logs<br>► ePO agents | ► ePO agents<br>► DNS<br>► NetFlow<br>► Proxy logs (web)<br>► Proxy logs (email)<br>► Email logs | ► FTP logs<br>► Proxy logs (web)<br>► Proxy logs (email)<br>► Email logs<br>► DNS |

# Breach Investigation

- Conducting a Security Breach Investigation
  - Who attacked us?
  - What was targeted?
  - When did the various events occur?
  - From where did the attacks come?
  - Why did they attack?
  - How did they get in, stay in and get the data out?
- Evidence Handling
- Safeguarding and protection the investigation

# Security Risks in Outsourcing/Vendors

- Perimeter controls will not protect us against mobile computing, data sharing with **external parties and service providers.**

- Require **3rd party security risk framework**

  Key components:
  - Structure and governance model
  - Contractual requirements
  - Assessment of risk:
    - Type of service provider
    - What data do we share?
    - What are their controls related to the data?
    - 4th party involvement?

# Cybersecurity Awareness Training

- Cybersecurity awareness training
- Cybersecurity technical training
- …

**Cyber technical training**

**Information security user awareness training**

DOs &
DON'Ts

# DON'Ts

- **DON'T** left the **removable devices unprotected**
- **DON'T** install **cracked/ patched software**
- **DON'T turn-off the antivirus software** in computers

- **DON'T save password** in web browsers and applications
- **DON'T click** on **pop-up windows** when surfing internet
- **DON'T click on links** or **open attached files** in suspicious emails
- **DON'T respond** to emails that request **confidential** information

# DOs

- **Log out** computer when unattended
- **Set password** for files before sending to public channels
- **Check source** of incoming email for authentication

- **Shred** confidential hard-copy documents when no longer used
- **Report suspicious security incidents** to IT Risk/ Information Security Department

# Q&A

Building a better working world

# EY Vietnam contacts

**Henri Hoang**
Cybersecurity Leader - Partner - EY Vietnam
**henri.hoang@vn.ey.com**

**Dung Nguyen Bui**
Cybersecurity Senior Manager
**dung.nguyen.bui@vn.ey.com**

**Kiet The Nguyen**
Cybersecurity Manager
**kiet.the.nguyen@vn.ey.com**

See the full thought leadership report:
**Creating trust in the digital world –**
EY's Global Information Security Survey 2015
www.ey.com/GISS2015

View more of EY's insights on cybersecurity on:
www.ey.com/cybersecurity

**EY** | Assurance | Tax | Transactions | Advisory

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and/or one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

©2016 Ernst & Young Vietnam Limited.
All Rights Reserved.
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

**ey.com**