OWASP
Open Web Application
Security Project

Achilles and the Bee

A façade of infallibility

About me…

Fabiola Amedo

IT Advisory practice @ KPMG

What I do:

- IT controls testing
- Info Sec standards Implementation
- Vulnerability Assessments and Pen Tests

Fun facts:

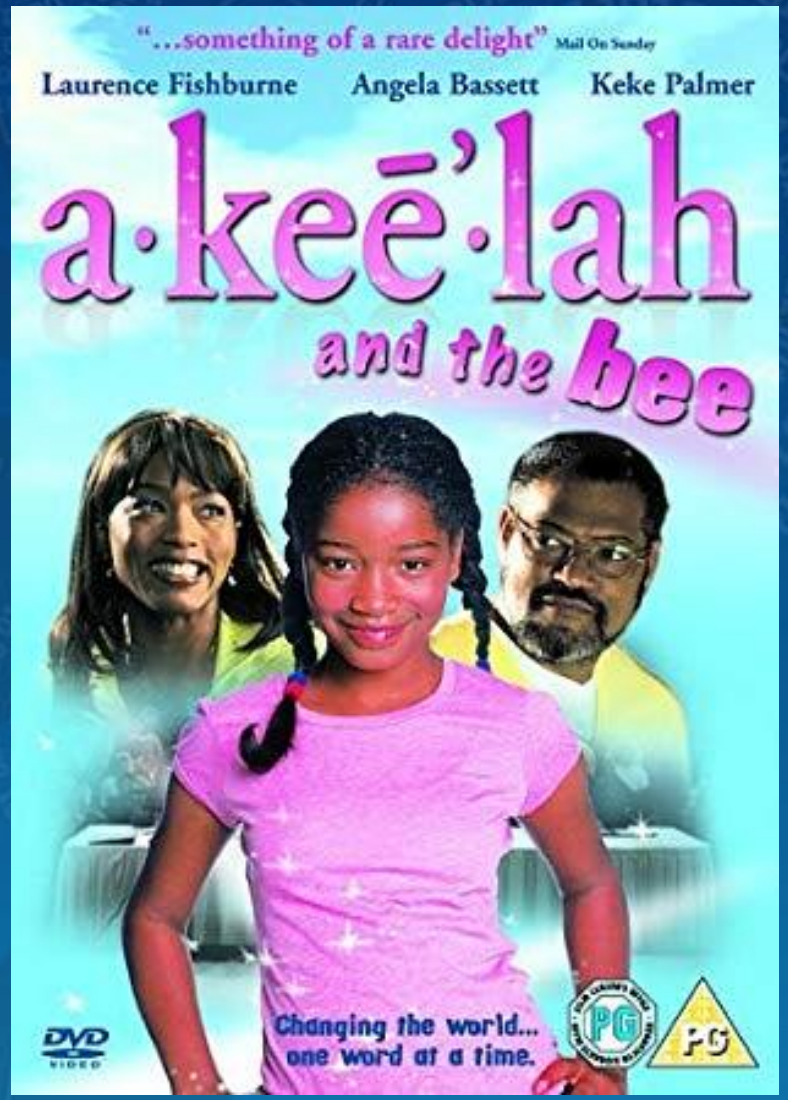
- I love sports (actively involved in football-watching and cycling)
- Closet writer (looking to publish soon) - tech fiction, other genre and poetry
- Et je parle français au niveau intermédiaire aussi

OWASP
Open Web Application Security Project

You're probably wondering what this presentation is about right…?

Well, it's not about a movie…

It's all about cyber security!!! ☺



OWASP
Open Web Application Security Project

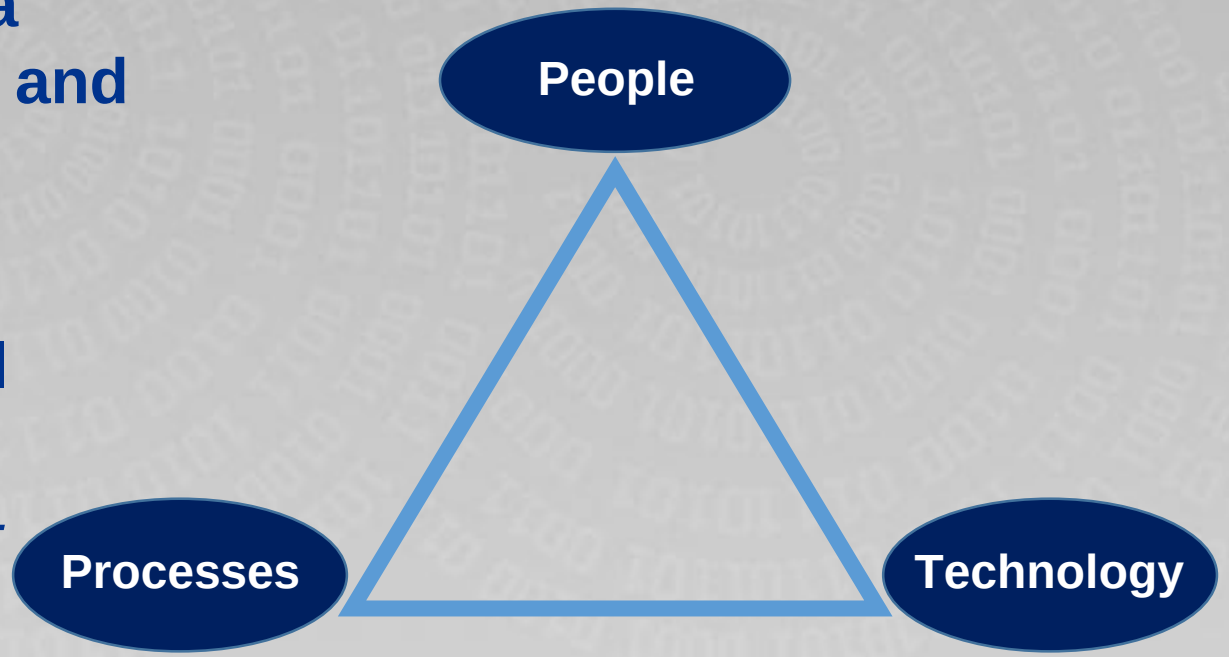
How many of you know the story of Achilles?

What we know…

Managing Information Security is a combination of People, Processes and Technology.

Out of these 3, PEOPLE tend to be the weakest link - the Achilles heel

"There are many holes in the human firewall. Social engineering can bypass all forms of anti-intrusion technology" – Kevin Mitnick



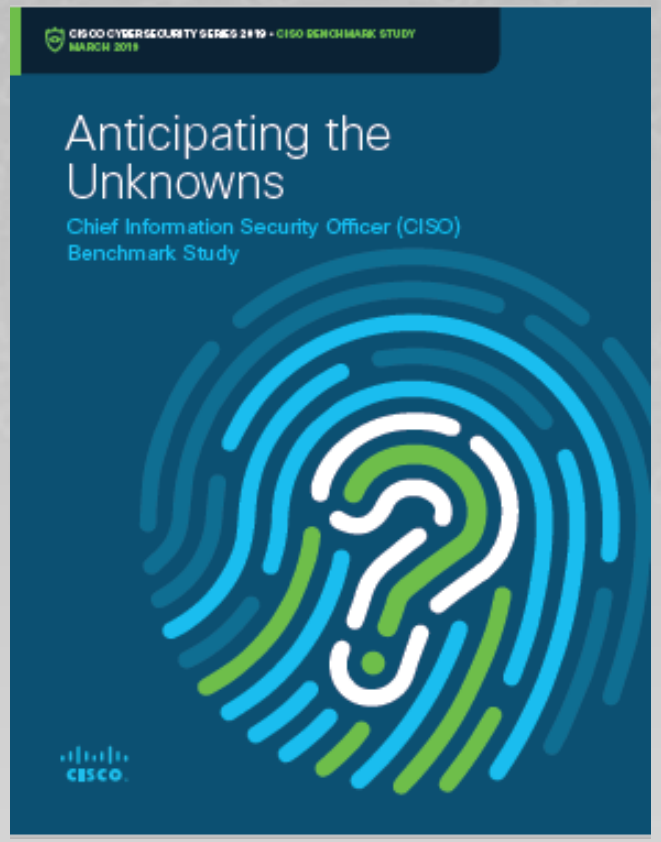
Yet…

Organizations we believe to have the most sophisticated technology are crippled by their "Achilles Heel"…

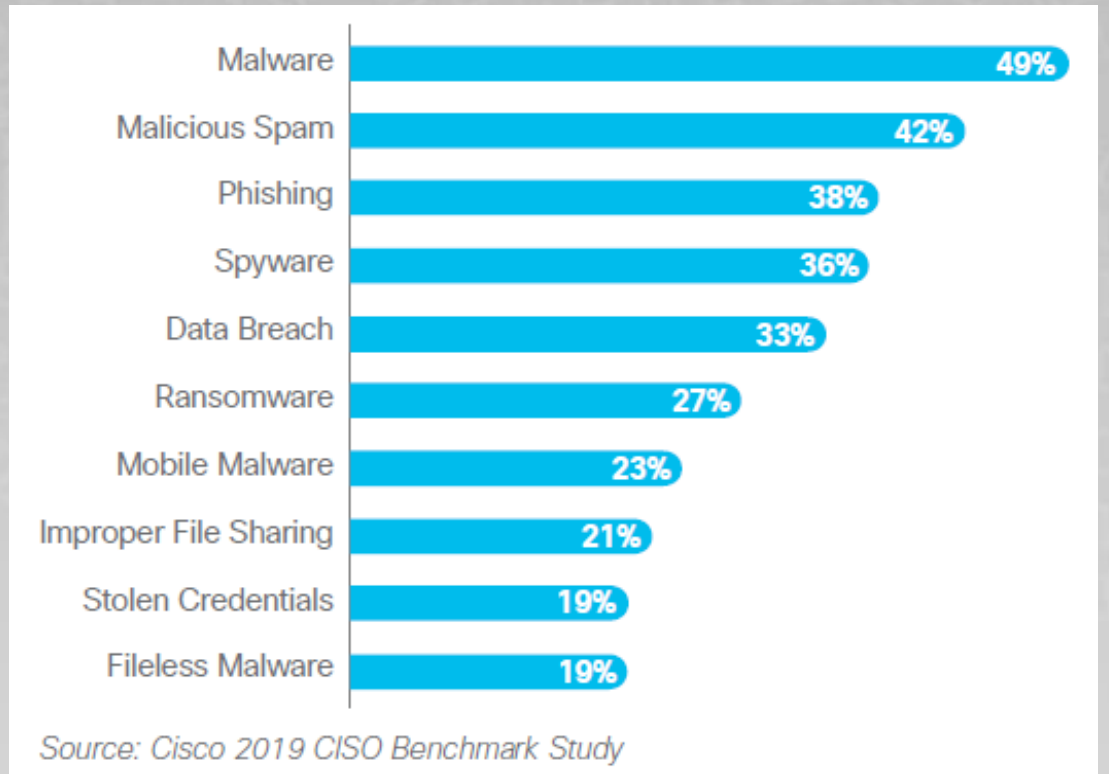
2011 **2013** **2014** **2016** **2018**

The effort and time these organizations spent in fortifying their systems were undermined by a single phishing/ social engineering incident…

2019 CISO Benchmark Report - CISCO



Which security incidents/ attack types have you encountered in the past year?



The **TOP 3** security incidents are issues with email security; which remains the #1 threat vector.

Ghana's threat landscape…

In Ghana…

2017

- Cyber criminals stole an estimated **$69.2 million** from corporate bodies, individuals and groups.
- Out of this amount, an estimated **$28 million (40%)** was stolen from banks in Ghana.

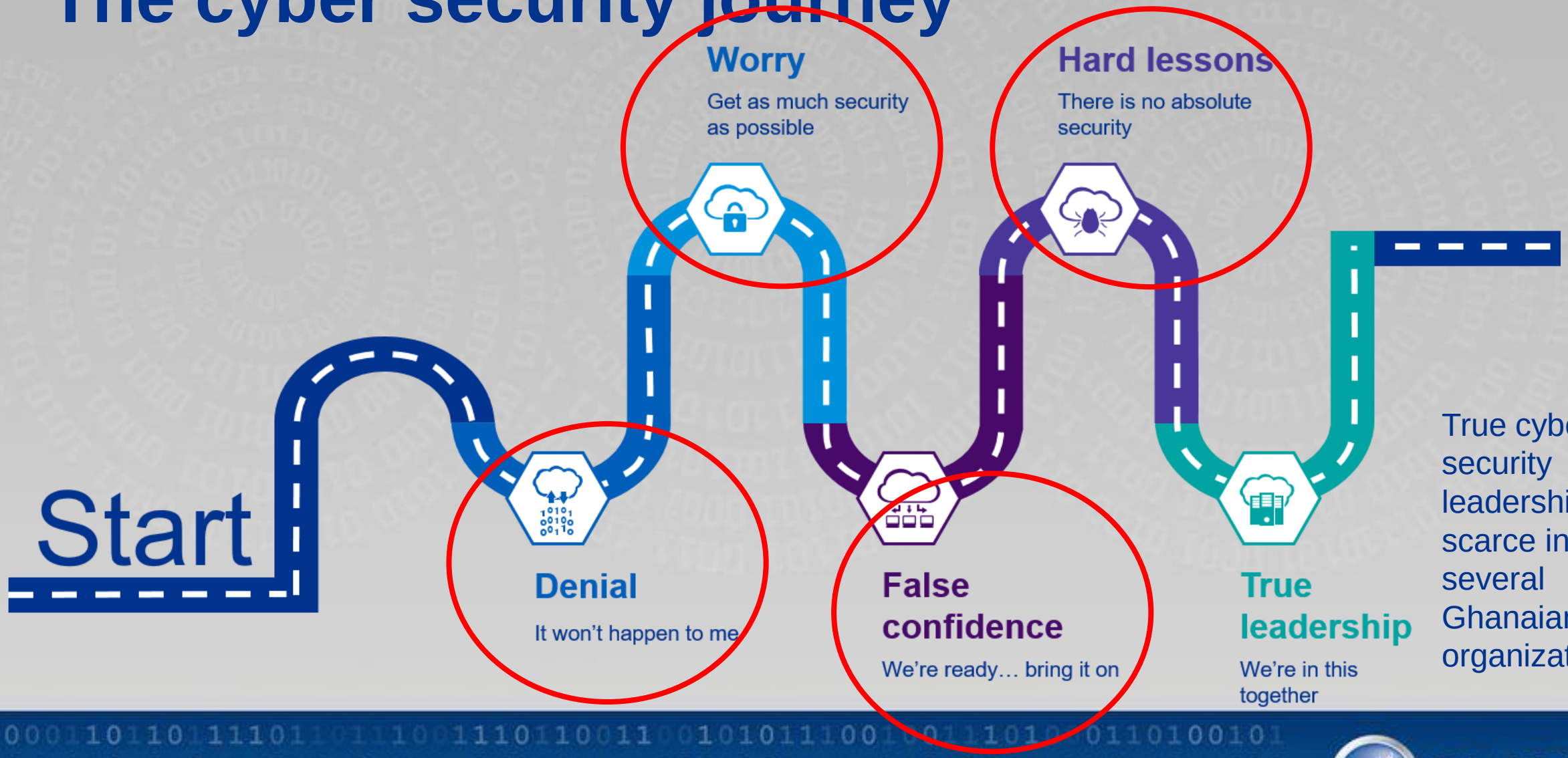
2018

- Losses increased to **$97 million**

Source:

Cybercrime Unit of the Criminal Investigation Department (CID)

The cyber security journey



True cyber security leadership is scarce in several Ghanaian organizations.

What I have learnt over the years…

- Every organization has an **Achilles Heel**
- Organizations tend to spend huge sections of their IT budgets on new technology and security: e.g. wave of digital disruption
- Some companies are still making IT (day-to-day) people focus on security.
- In Ghana, several organizations are still not doing enough when it comes to security… imbalance and isolation between people, technology and processes.
- Companies are focused on buying “solutions” to solve problems but forget to fix the **“LITTLE”** things
- Low optimization: Poor configuration of sophisticated solutions

What can be done?

As cliché as it sounds, defending against these kinds of attacks (phishing & other social engineering attacks) requires a coordinated and layered approach to security:

- Constantly train employees so that they recognize phishing attacks and avoid clicking malicious links. Organize training that actually works and measure it to know the impact.
- Using SPAM filters that detect viruses, blank senders, etc.
- Using **2FA*** and U2F (Universal 2nd factor authentication supplements 2FA)
- Deploy a good Antivirus solution (schedule and monitor signature updates)
- Blocking malicious sites through web filtering
- Encrypt!

*** Now it's possible to bypass 2FA using new tools such as Muraen and NecroBrowser. They can automate and bypass 2FA by stealing session cookies.

OWASP
Open Web Application
Security Project

Easily overlooked vulnerabilities

Open Relay Vulnerability

When an email server is configured to accept emails from any sender and deliver it to any recipient. This vulnerability can be easily overlooked and exploited by malicious users from within and outside the organization. Executed with simple commands as follows:

telnet mail.owaspmail.com 25
Connected mail.owasp.com
220 mail.owaspmail.com
HELO owasp.com

MAIL FROM: <dosei@owasp.com>

RCPT TO: <trudy@owasp.com>

DATA

Dear Mr. Finance Officer, credit A/C number 00012345670 with an amount of $100,000. MD.
.

Open Relay Vulnerability

Fixes

- Configure the email server to receive e-mails for your domain and your domain only
- If you're using Exchange 2007 or Exchange 2010 server with an Open Relay, you can run a simple command from the Exchange Management Shell to fix it:

  "Get-ReceiveConnector "YourReceiveConnectorName" | Remove-ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "ms-Exch-SMTP-Accept-Any-Recipient"

- For Exchange 2013 onwards, there is guidance on how to fix this at support.microsoft.com

Phishing Campaigns

Identifying a cloned site:

- Look for a padlock symbol in the address bar and check that the URL begins with a 'https://‘
- Consider the spelling of the web address : e.g. yahoo.com can easily be changed to yah00.org owasp.org -→ 0wasp.org
- Check the content and “look and feel” of the page. At most times phishing sites look sub-standard. Also look for misspelt words and urgent action required.
- Conduct a ‘WHOIS’ look up to see who owns the website using free online query tools e.g. network-tools.com
- Check the website creation date. If the website has not been around for a long time (a few months) you should start to suspect it.
- Check the payment methods e.g. card payment. Legitimate websites will not ask you to make bank transfers.

The Bee part of this presentation…

Honey Pots

Fun fact:

Bees and hornets are sworn enemies. To defend themselves when hornets invade the colony, the bees surround them and can generate temperatures up to about 47ºC which can kill the hornets.

Nature possesses some of the most sophisticated defence mechanisms.

We can look to nature for inspiration in developing information security solutions.

Honey Pots

- A security mechanism used to detect and thwart the attempts of hackers
- Appear to be poorly secured
- Honey pots help organisations design more secure systems
- Essentially an effective method for tracking hacker behaviour and helps heighten the effectiveness of computer security tools.

References

- https://support.microsoft.com/en-us/help/324958/how-to-block-open-smtp-relaying-and-clean-up-exchange-server-smtp-queu
- https://support.symantec.com/en_US/article.HOWTO126073.html
- https://www.cisco.com/c/en/us/products/security/security-reports.html#~cybersecurity-report
- https://www.cybersecuritymastersdegree.org/2017/11/top-5-social-engineering-attacks-of-all-time/
- https://news.nationalgeographic.com/news/2012/03/120316-hot-bee-balls-hornets-insects-brains-animals-science/
- https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#6af91649546f
- https://www.ghanaweb.com/GhanaHomePage/business/Ghana-loses-US-97m-in-2-years-to-cyber-fraud-695556

OWASP
Open Web Application
Security Project

Thank you

Contributions and Questions are welcome