

هيئة المعلومات
والحكومة الإلكترونية



INFORMATION &
eGOVERNMENT AUTHORITY

The Soft War in Bahrain

Hacker Success Stories

Ahmed Jaber Aldoseri

Director General of Information Security & Radiocommunications

21st September 2016

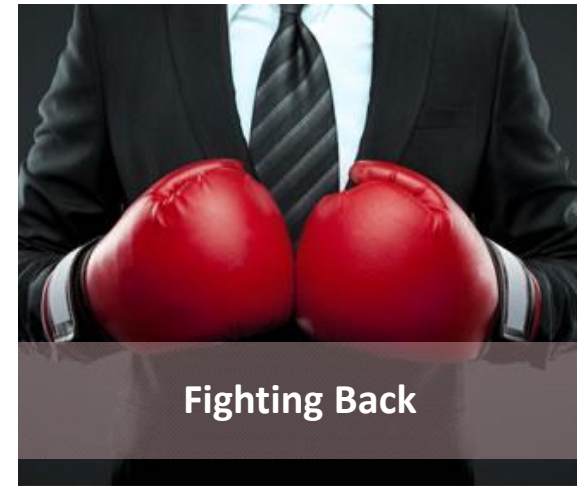


INFORMATION &
eGOVERNMENT AUTHORITY

External Document



Agenda

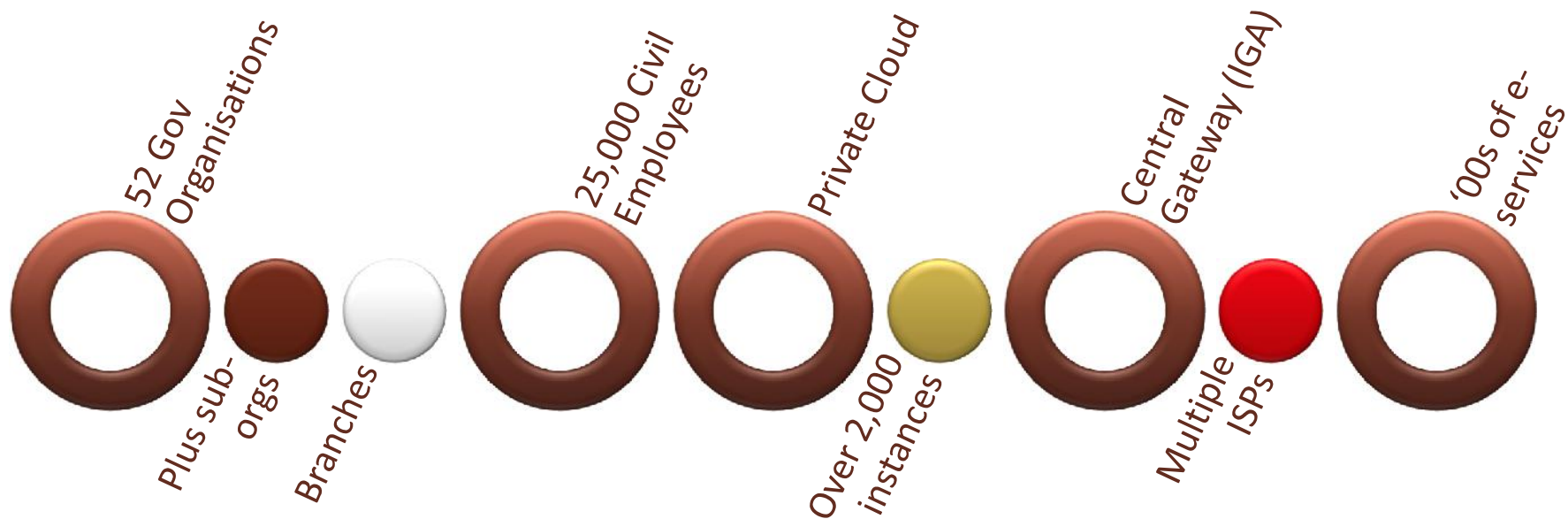




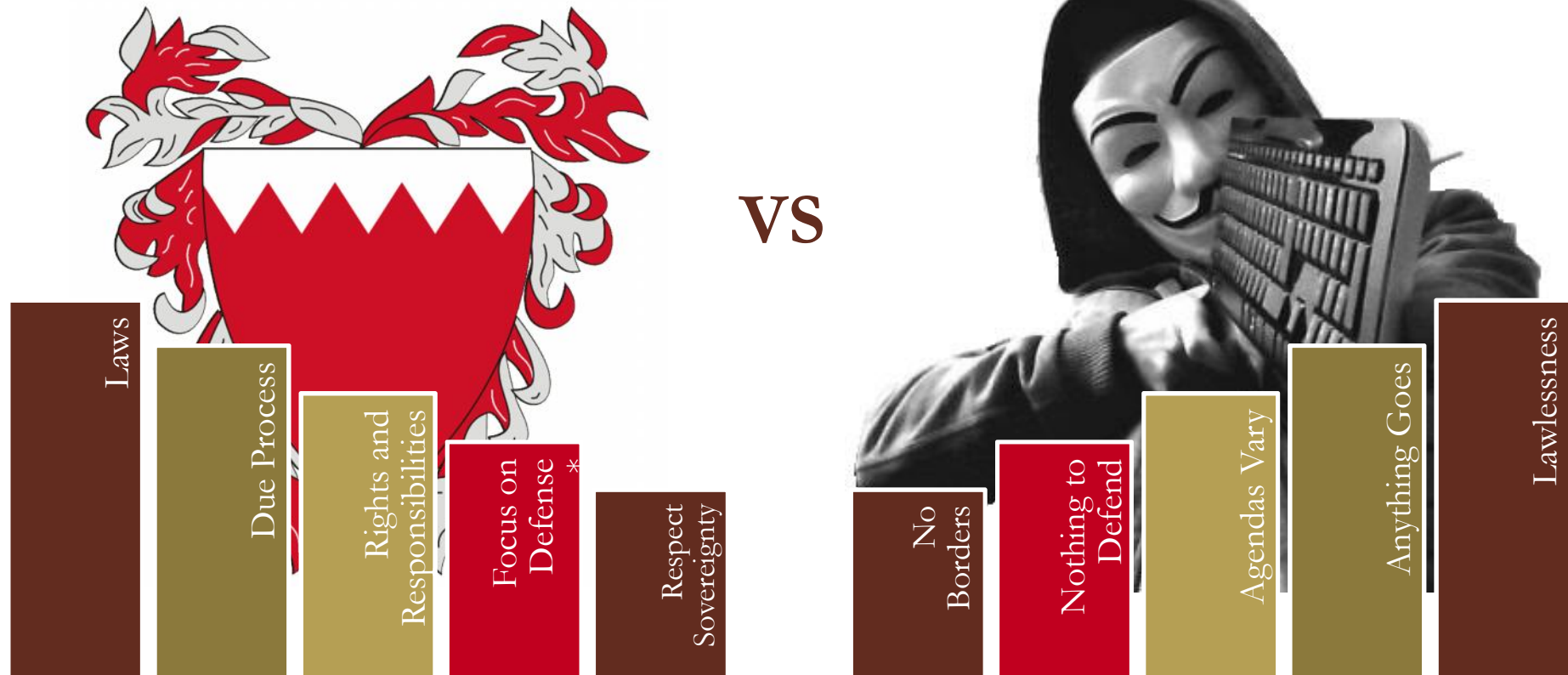
Current Threat Landscape



The Assets

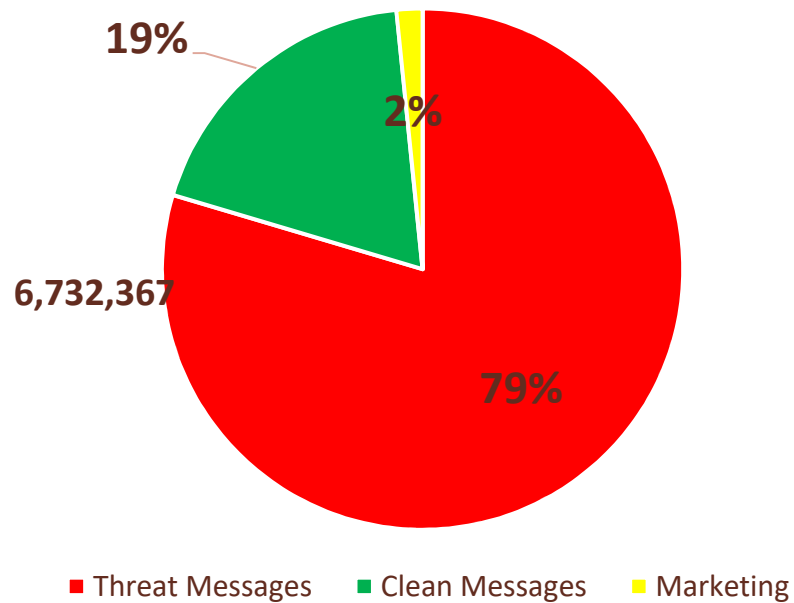


The Playing Field

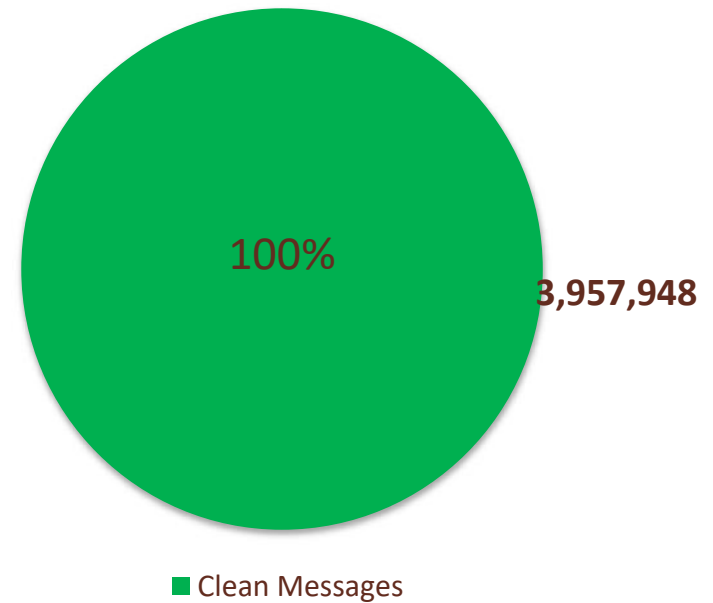


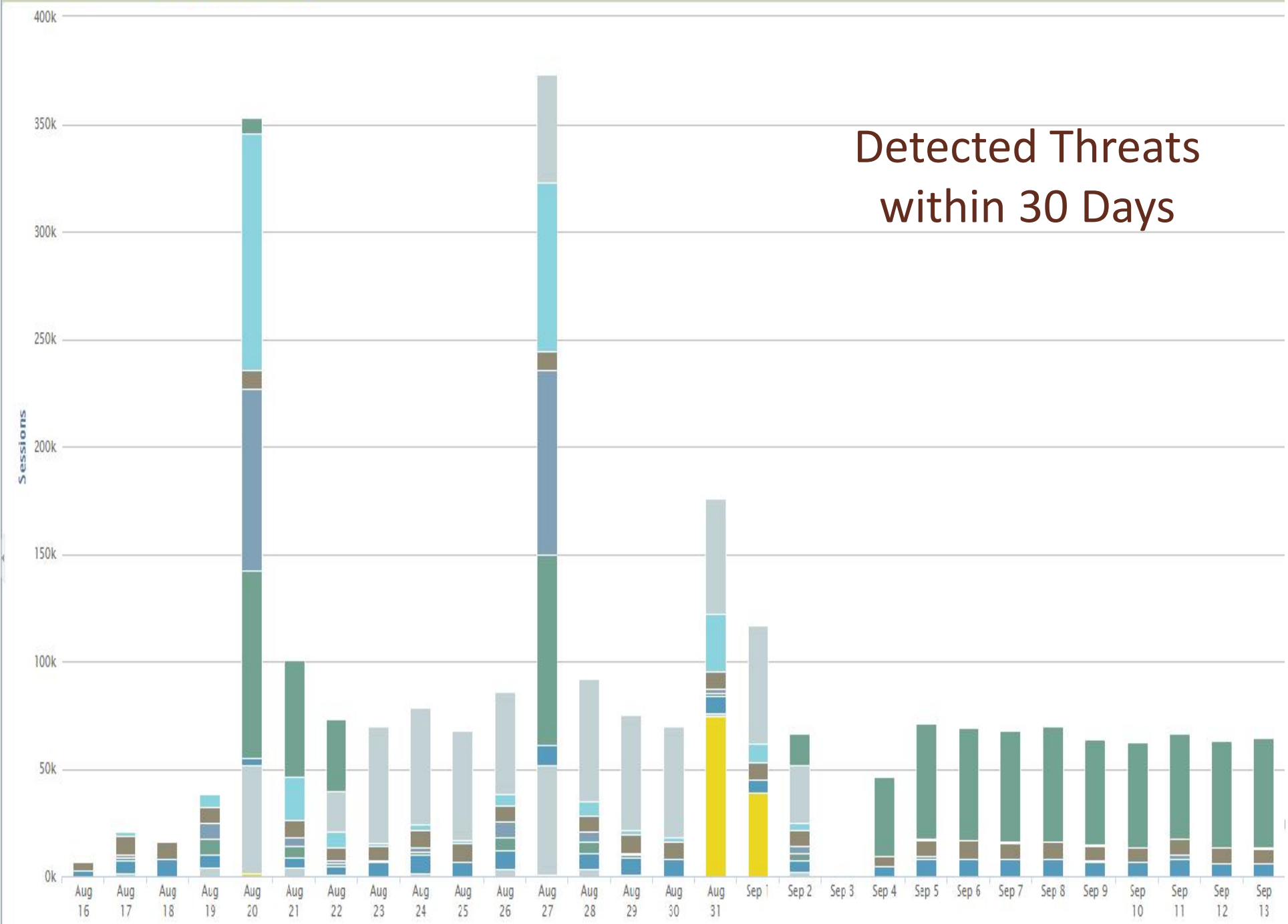
A Typical Month's Traffic

Incoming Email

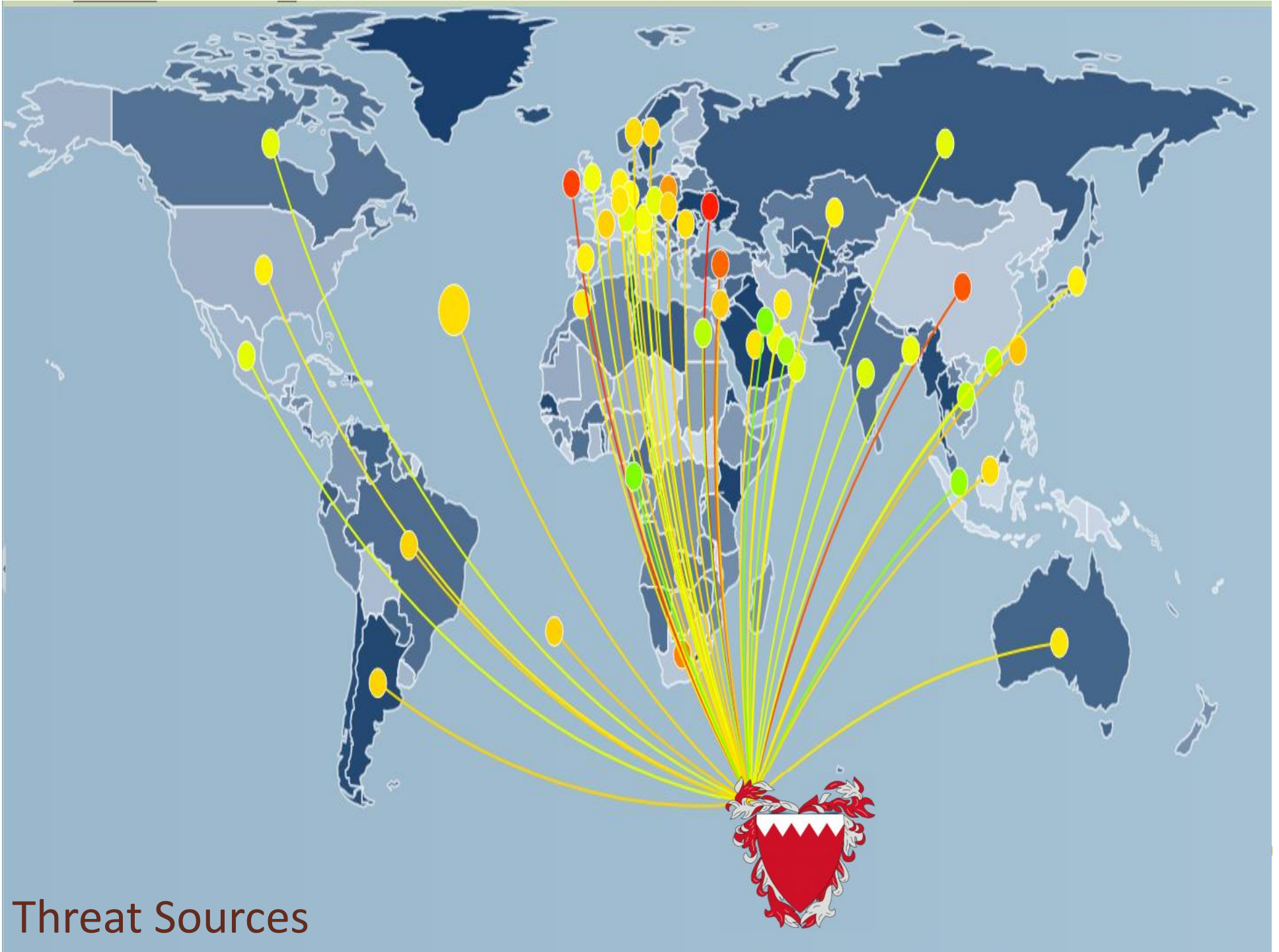


Outgoing Email





Detected Threats within 30 Days



Threat Sources

Zooming in...



China

- Over 100K threats
- Overall risk 4.2/5



Ukraine

- 1 Attack
- Risk Rating 4.7/5.0!

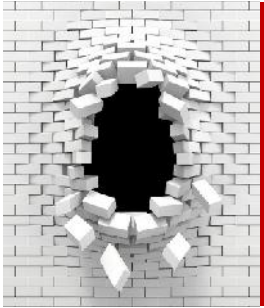




How many threats were
undetected?

“We don’t know what we don’t know!”





Successful Intrusions Against Bahraini Targets

Stories from the CERT.bh Forensics Lab

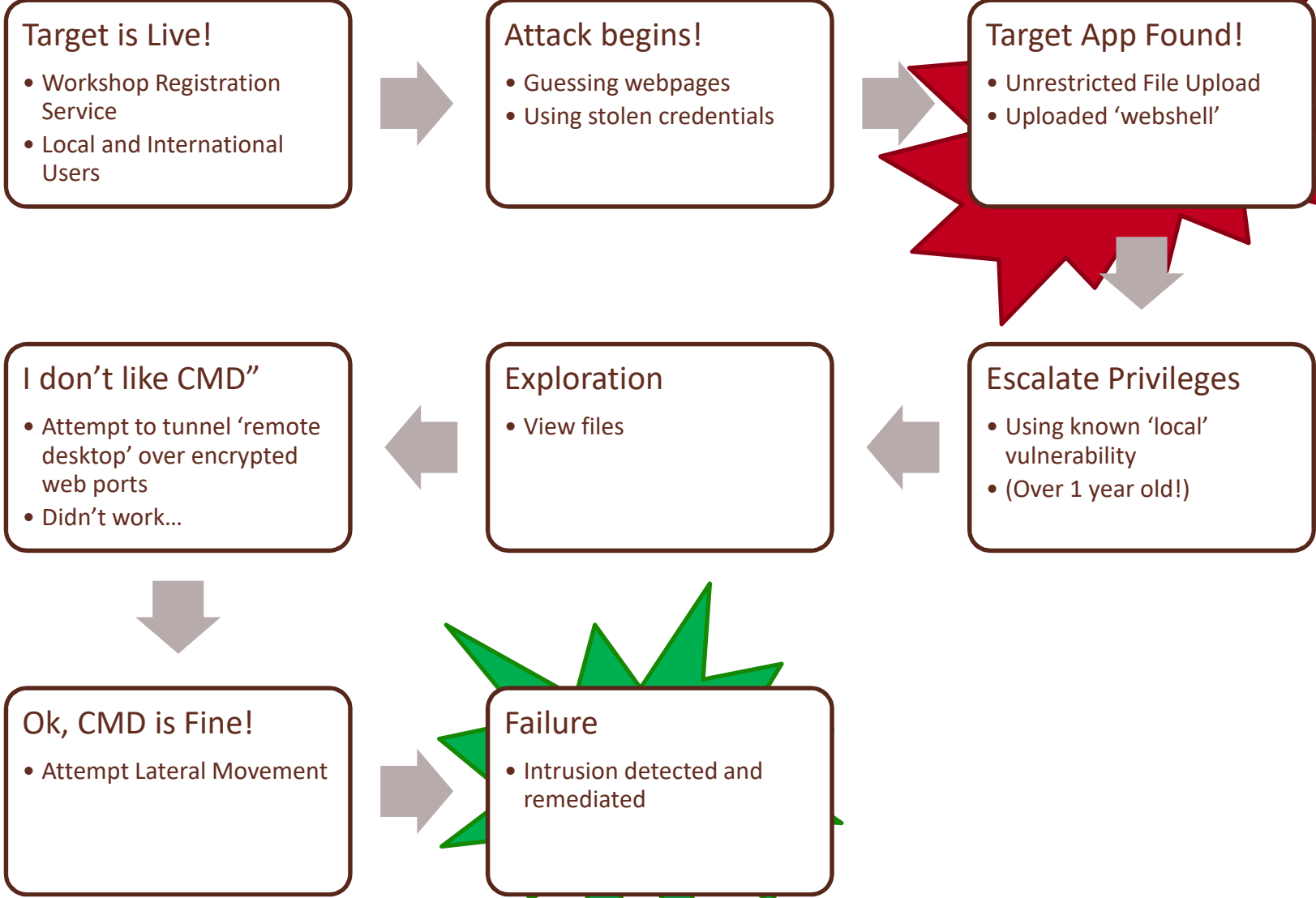


INFORMATION &
eGOVERNMENT AUTHORITY

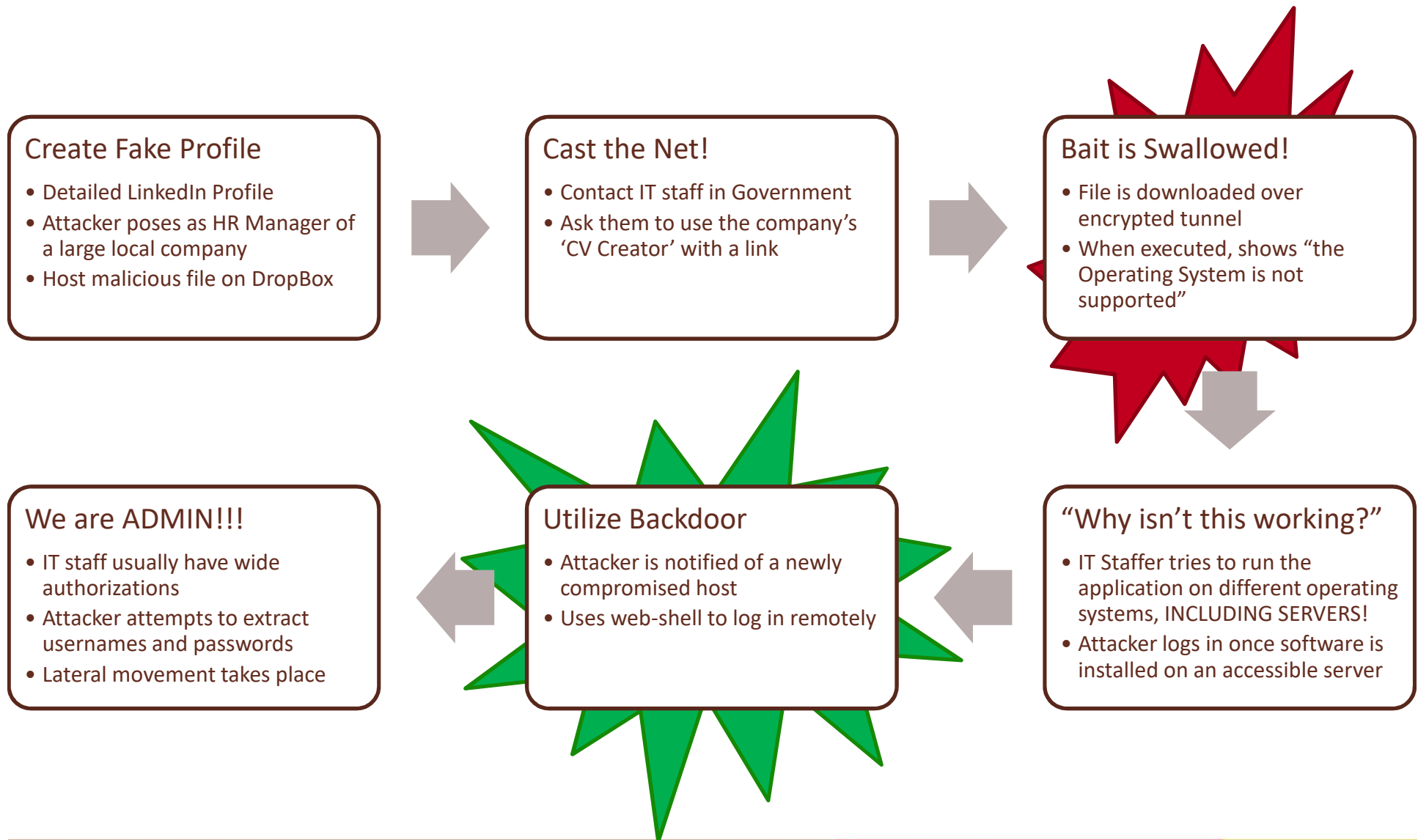
External Document



Case 1: Unrestricted File Upload



Case 2: Humans are the Weakest Link



[- Tough Privileged Identity Negative Audit Findings Solved in Hours-See H](#)



Mohammed AlHammad

Human Resources Officer at [REDACTED]



Jan 2

Hi ...

The company that I have worked for now ([REDACTED] Telecommunications Service Provider), started a new phase of Recruitment process to Recruit some professional People to work for them.

I saw your Skills and Experience in your page and I think you are suitable for some positions in our company Also as I know [REDACTED] provides a lot of Advantages for staffs. Like Help To Learning Some new Skills and Academic Educations, High and Good Salary, Cool and safe job position and etc.

If you are interested to join us , you can send to me your cv with our special cv creator program.

you can download this program from this link

[https://www.dropbox.com/s/\[REDACTED\]](https://www.dropbox.com/s/[REDACTED])

and file password is [REDACTED]

my personal email is: Md.AlHammad@outlook.com

Best Regards

11:45 AM





Fighting Back





People



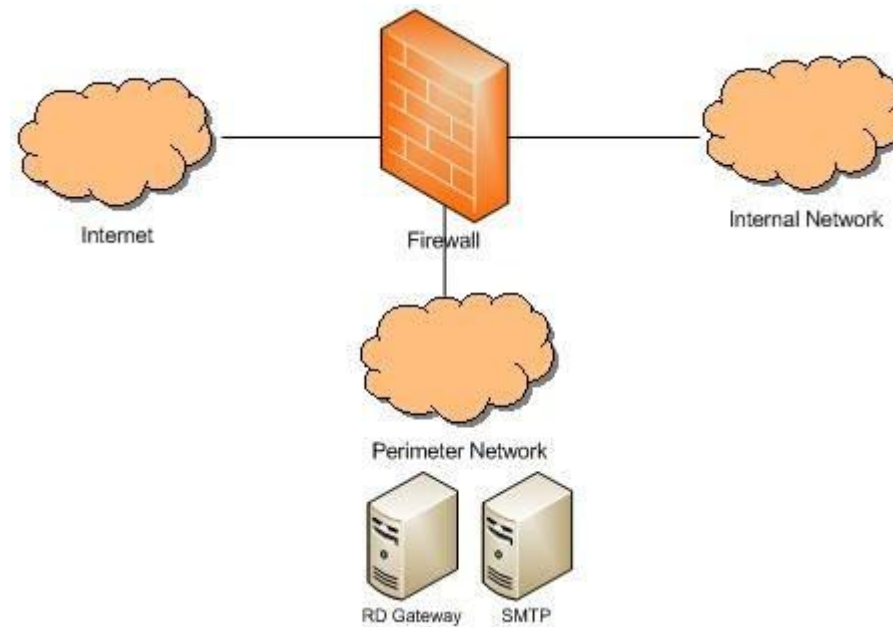
Technology



Processes



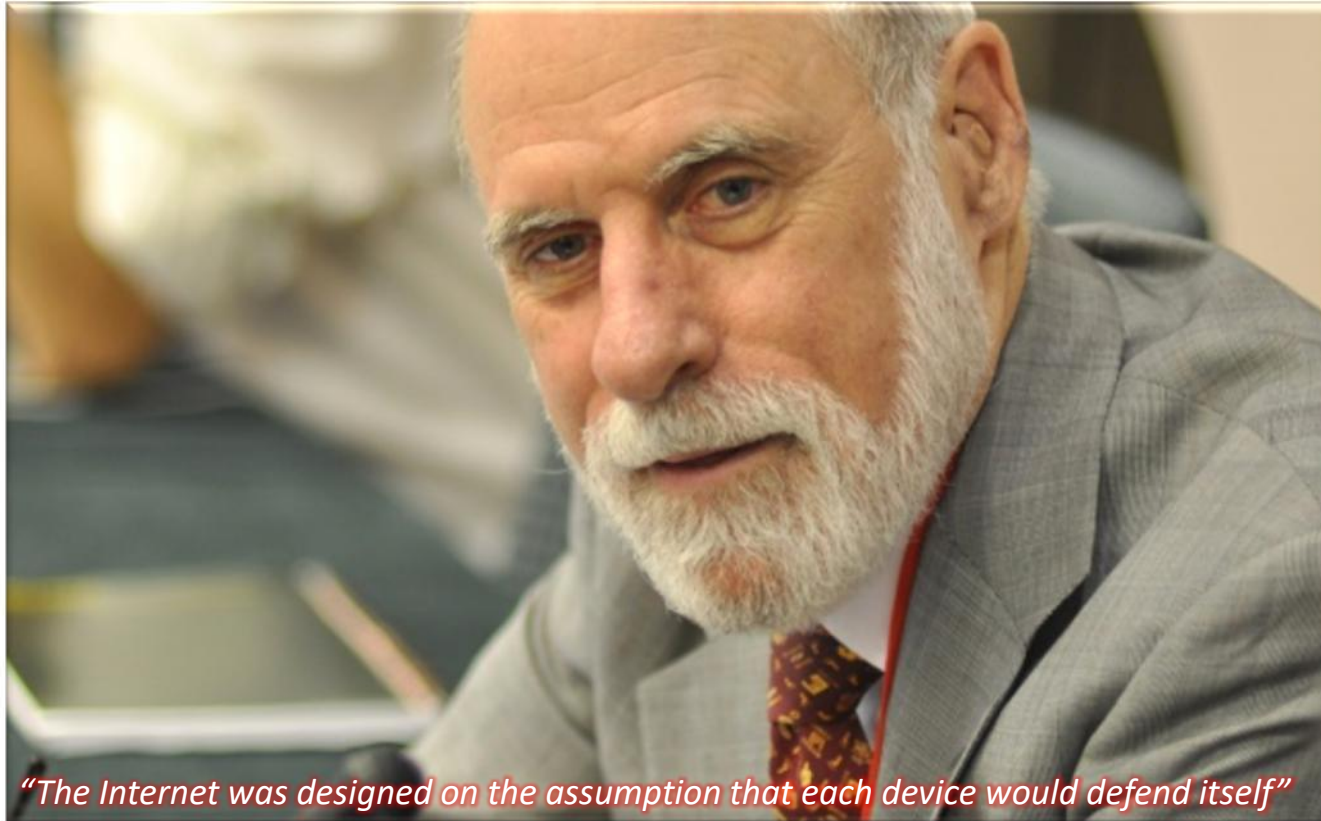
The classical network setup



Doesn't work any more...



TCP/IP Architecture History...

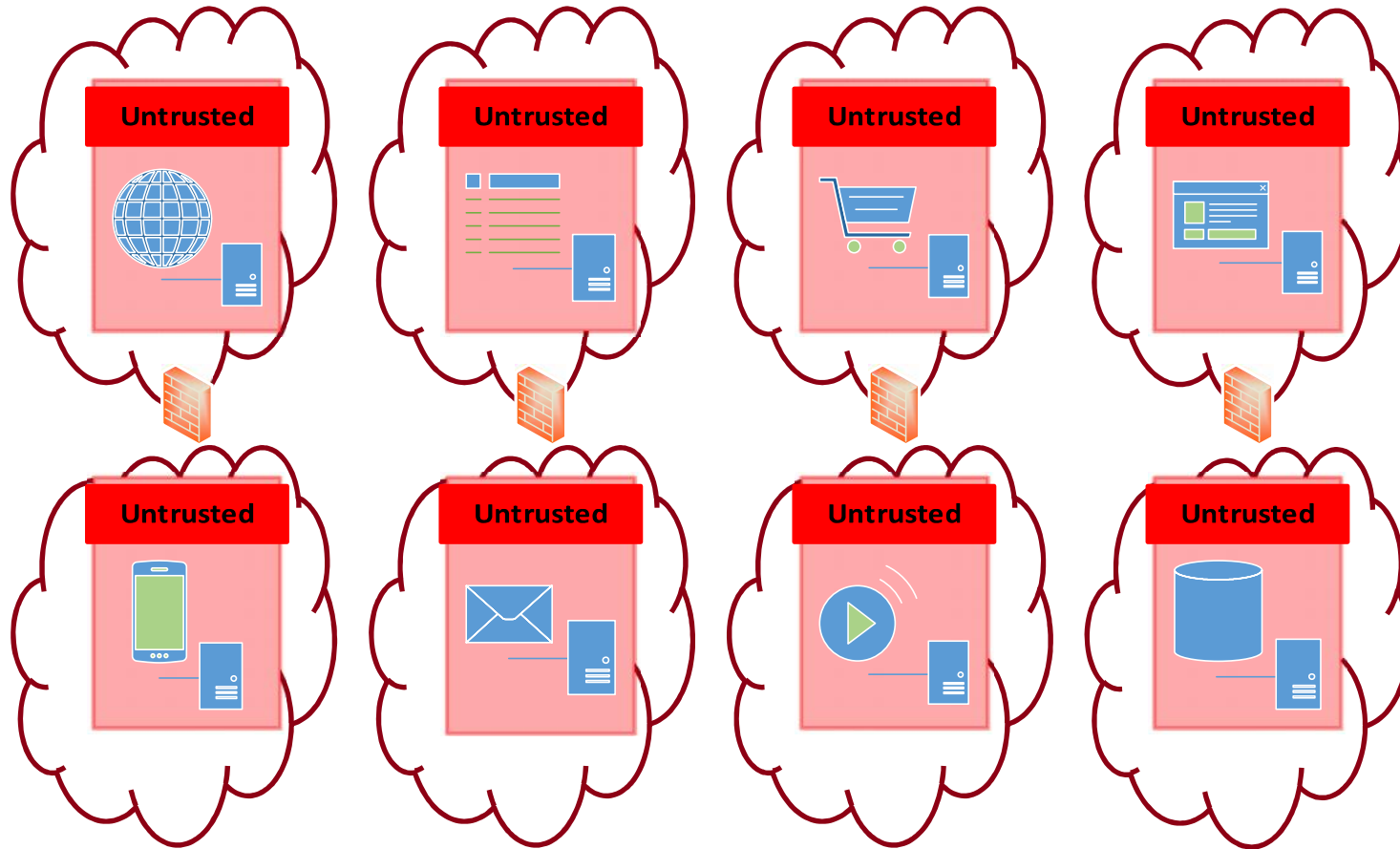


"The Internet was designed on the assumption that each device would defend itself"

Vint Cerf, Co-Inventor of TCP/IP, quoted at the CRCC 2015 meeting, May 2015, Washington DC



The Micro-Perimeter Design



Virtualization is key to the micro-perimeter design





Thank You

Ahmed Jaber Aldoseri

Director General of Information Security & Radiocommunications

AHMED@ALDOSERI.ORG



INFORMATION &
eGOVERNMENT AUTHORITY

External Document

