

CYBER SECURITY AN AVIATION PERSPECTIVE

Tony Vizza

ABOUT TONY

- 20+ Years Cyber Security Experience
- B. Science (Computer Science) – UTS
- Global Executive MBA – USYD / Stanford / LSE / IIMB
- CISSP - (ISC)²
- CRISC, CISM - ISACA
- ISO-27001 Lead Auditor (PECB)

In Progress:

Juris Doctor (UNSW)

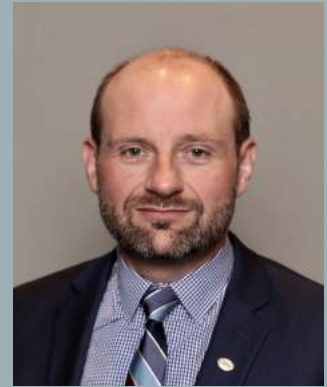
CCSP (ISC)²

ISO-27001 Senior Lead Auditor (PECB)

And Then:

CISSP-ISSMP (ISC)²

CIPP/E (IAPP)





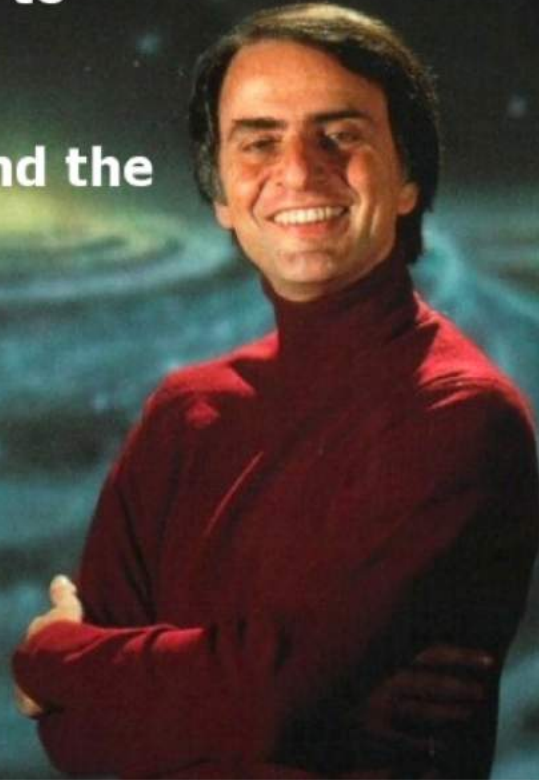
HOUSTON, WE HAVE A PROBLEM....

- 178 million records exposed in 2017 (US)
- 44.7% increase on 2016, a record year (US)
- Cybercrime now the second most reported crime in the world
- Cybercrime over 50% of all crime in the UK



**You need to
know the
past to
understand the
present**

~ Carl Sagan ~

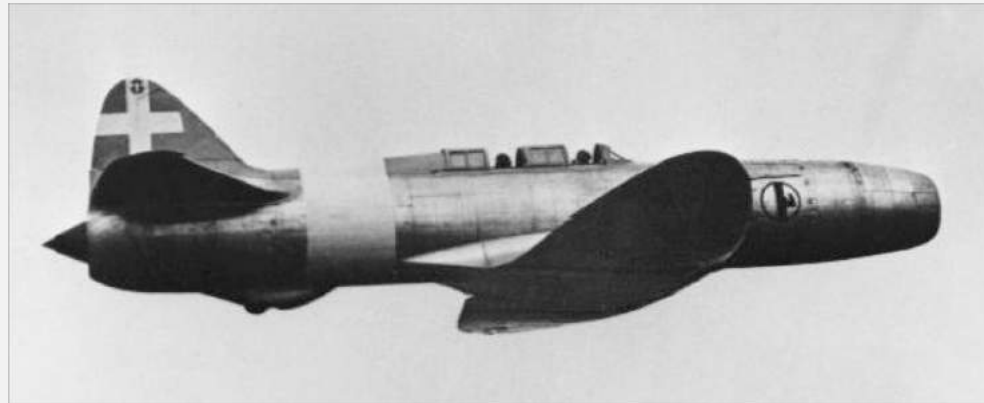












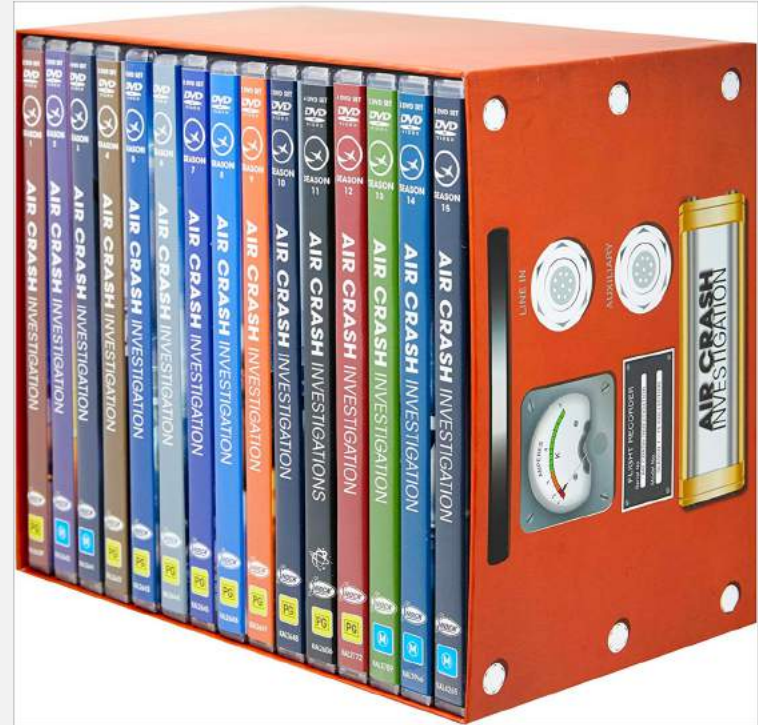


39,897
km/h

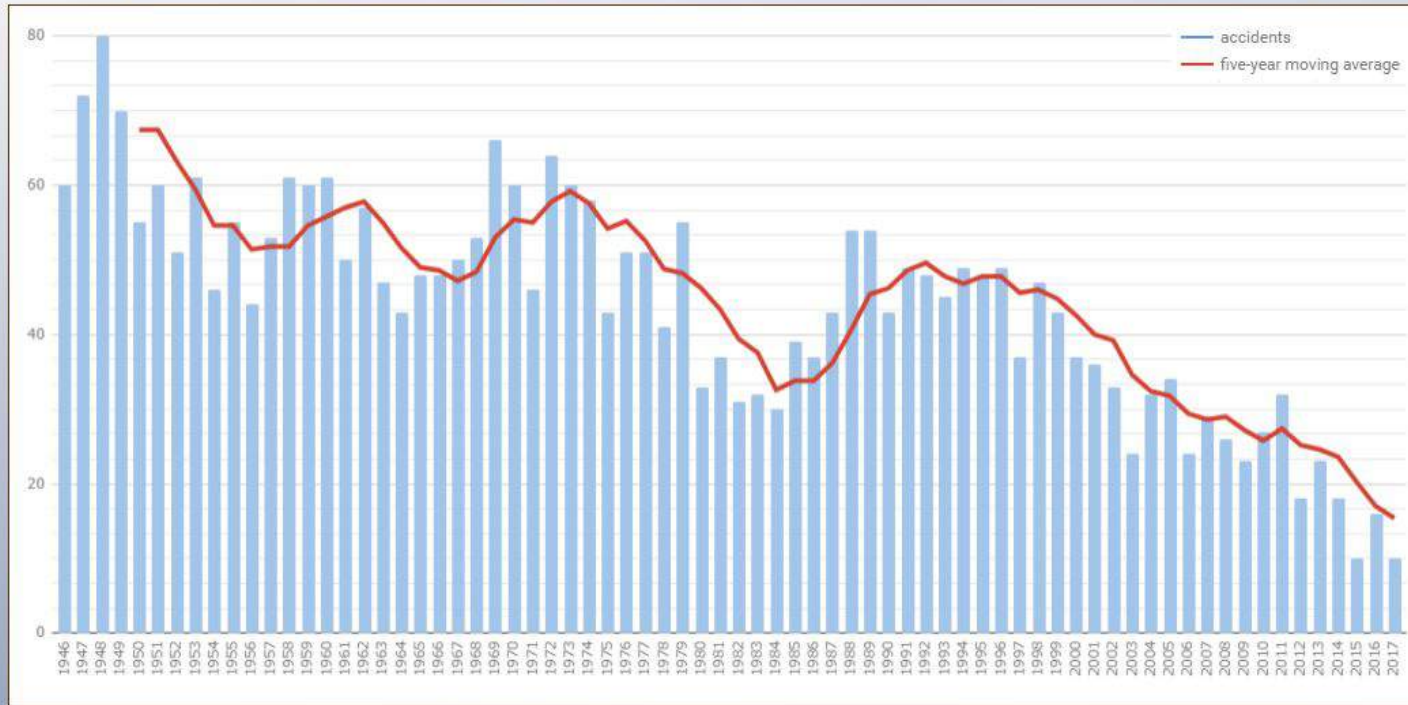








Fatal Airliner Accidents Per Year 1946-2017



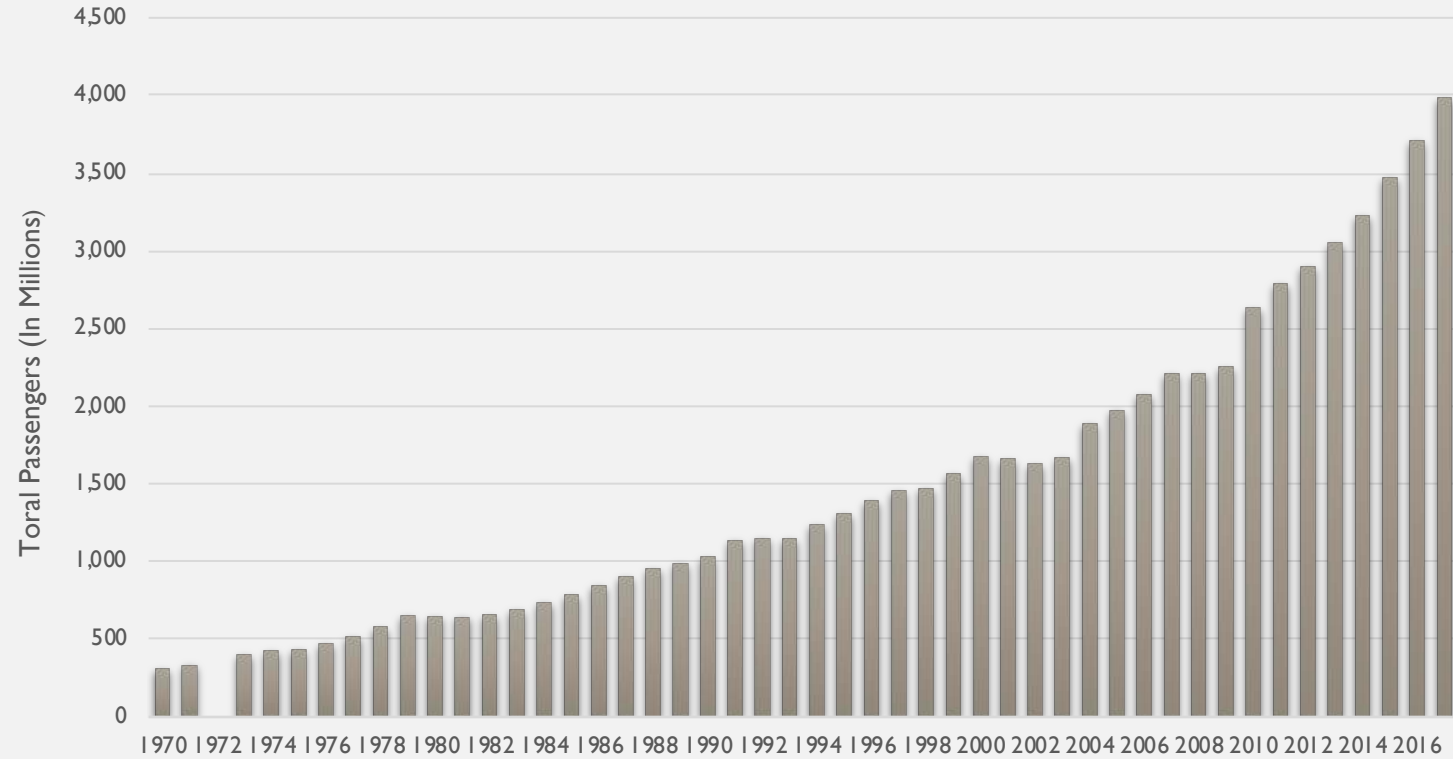
Statistics are based on all worldwide commercial (cargo and passenger) fatal accidents involving civil aircraft with a minimum capacity of 14 passengers, from the ASN Safety Database <https://aviation-safety.net>



Aviation**Safety**Network

Air Transport, Passengers Carried

Source - International Civil Aviation Organisation (ICAO)







BEFORE START

COCKPIT PREP	COMPLETE
GEAR PINS and COVERS	REMOVED
SIGNS	ON
ADIRS	NAV
FUEL QUANTITY	KG
TO DATA	SET
BARO REF	SET

WINDOWS/DOORS	CLOSED
BEACON	ON
THR LEVERS	IDLE
PARKING BRAKE	AS RORD

AFTER START

ANTI ICE	AS RORD
ECAM STATUS	CHECKED
THR LEVERS	IDLE
PARKING BRAKE	AS RORD

BEFORE TAKEOFF

FLIGHT CONTROLS	CHECKED
FLIGHT INST	CHECKED
BRIEFING	CONFIRMED
FLAPS SETTING	CONF - SET
V1 VR V2 / FLEX TEMP	SET
ATC	SET
ECAM MEMO	TO ALL GREEN

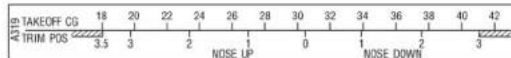
CABIN CREW	ADVISED
ENG MODE SEL	AS RORD
PACKS	AS RORD

AFTER TAKEOFF / CLIMB

LDG GEAR	UP
FLAPS	RETRACTED
PACKS	ON
BARO REF	STD

ON GROUND EMER EVACUATION

- AIRCRAFT / PARKING BRK. STOP/ON
- ATC (VHF 1). NOTIFY
- ΔP (only if MAN CAB PR has been used). CHECK ZERO
- if not zero, MODE SEL on MAN and VIS CTL FULL UP*
- ENG MASTER 1 and 2. OFF
- CABIN CREW (PA). NOTIFY
- FIRE P/Bs (ENG and APU). PUSH
- AGENTS (ENG and APU). AS RORD
- EVACUATION. INITIATE


APPROACH

BRIEFING	CONFIRMED
ECAM STATUS	CHECKED
SEAT BELTS	ON
BARO REF	SET
MDA / DA	SET
ENG MODE SEL	AS RORD

LANDING

CABIN CREW	ADVISED
A/THR	SPEED / OFF
ECAM MEMO	LDG ALL GREEN

- LDG GEAR	ON
- SPOILER	ON
- CARRI. READY	ON
- SPOILER ARM	ON
- FLAPS	SET

AFTER LANDING

FLAPS	RETRACTED
SPOILERS	DISARMED
APU	START
PADAR	OFF / STBY

PARKING

APU BLEED	ON
ENGINES	OFF
SEAT BELTS	OFF
EXT LT	AS RORD
FUEL PUMPS	OFF
PARKING BRAKE and CHECKS	AS RORD

SECURING THE AIRCRAFT

ADIRS	OFF
OXYGEN	OFF
APU BLEED	OFF
EMER EXIT LIGHTS	OFF
NO SMOKING	OFF
APU and BAT	OFF









**REQUEST FOR
CRIMINAL BACKGROUND
CHECK**

Personal Information		First	Initial	Phone	State	City	Zip
Name (Last)							
Address (Mailing Address)							
E-Mail Address							
Services needed							





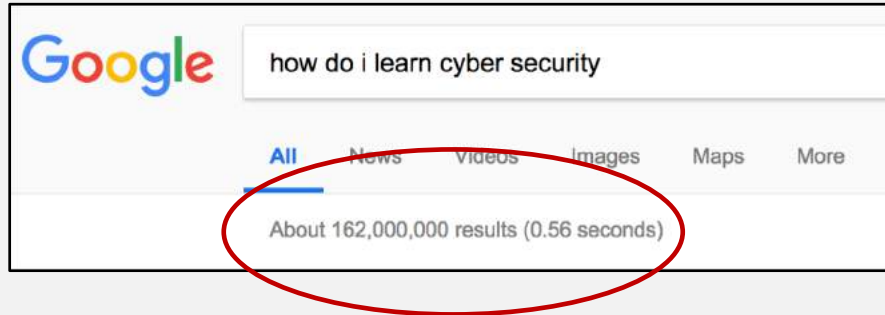
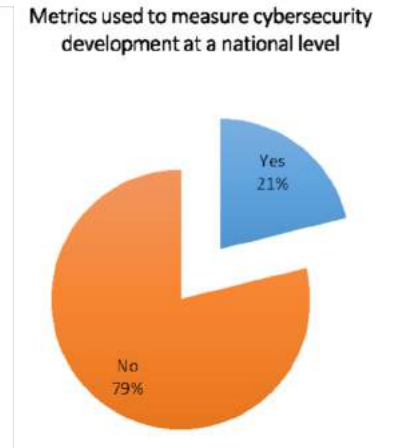
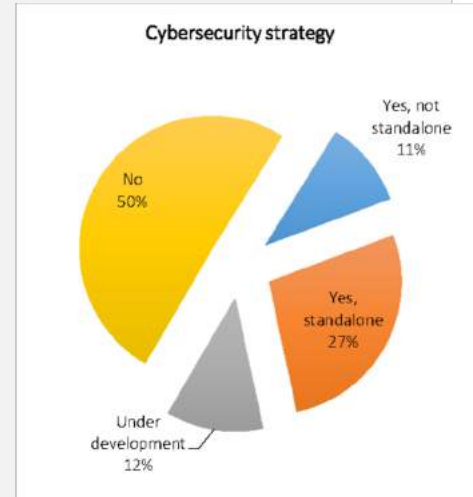
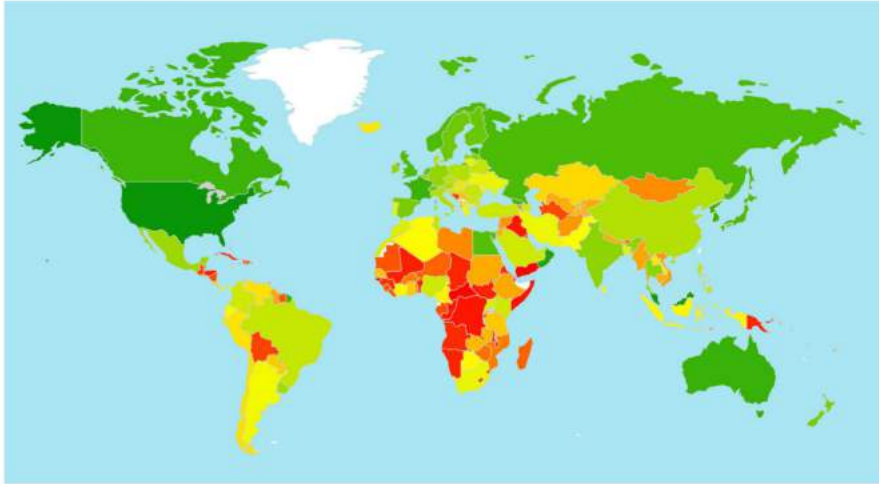
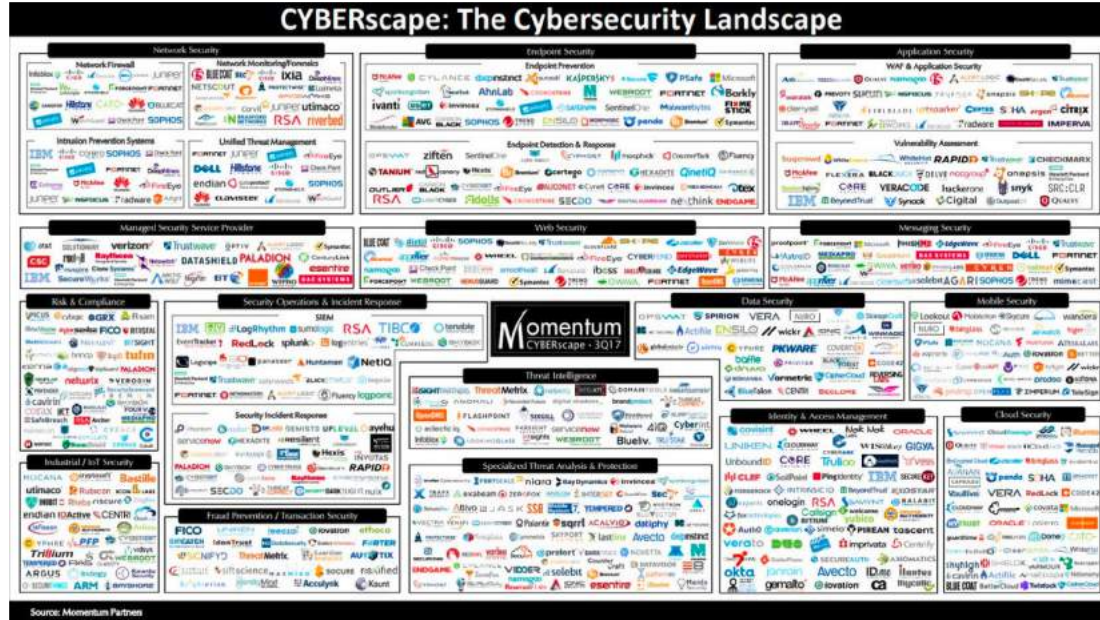
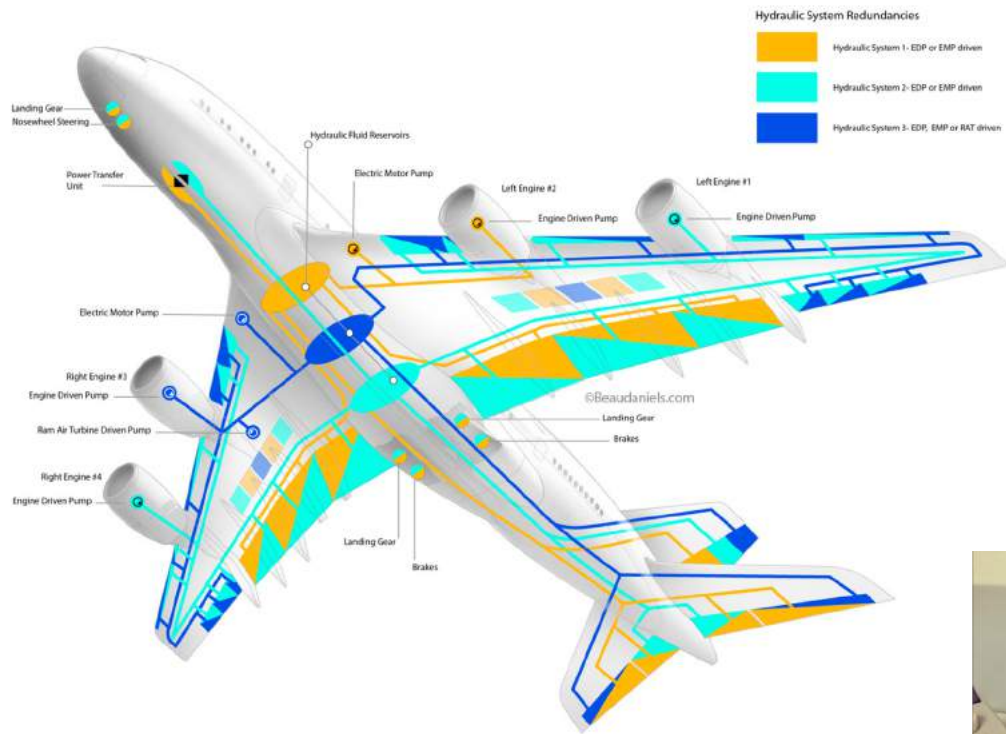


Figure 4.1.1: GCI Heat Map









10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.



User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.



Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.



Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.



Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Managing user privileges



Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management



Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring



Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working



Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk  [@ncsc](https://twitter.com/ncsc)





**CONVENTION
ON INTERNATIONAL CIVIL AVIATION**

Signed at Chicago, on 7 December 1944

**CONVENTION
RELATIVE À L'AVIATION CIVILE INTERNATIONALE**

Signée à Chicago, le 7 décembre 1944

**CONVENIO
DE AVIACIÓN CIVIL INTERNACIONAL**

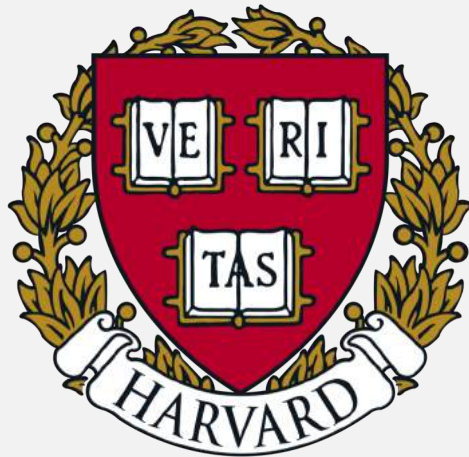
Firmado en Chicago, el 7 de diciembre de 1944

ICAO



OACI





4 Predictions for the Future of Cyber Security



1. We will reach agreement on international norms for how governments behave in cyberspace.



2. Governments will crack down on malicious cyber security within their borders.



3. Software companies will prioritize security.



4. We will all take more responsibility for practicing better cyber hygiene.







WHAT CAN WE LEARN FROM AVIATION

- Focus on Safety
- Training and Certification
- Flight Checks and Auditing
- Redundant Systems
- Regulated Operating Environment
- Automation

CYBER SECURITY

Why You Will (Probably) Never Being Unemployed.



Notifiable Data Breaches Quarterly Statistics Report

1 October – 31 December 2018

oaic.gov.au



OAIC

Final report issued: 7/02/19

**Table 1.A — Number of breaches reported under the Notifiable Data Breaches scheme by quarter
—All sectors**

Quarter	Total number of notifications
January to March 2018 * As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter	63
April to June 2018	242
July to September 2018	245
October to December 2018	262

Per the International Monetary Fund (2018)^[17]

Rank ↕	Country ↕	GDP (US\$million) ↕
	<i>World</i> ^[20]	84,835,462
1	 United States	20,513,000
	 <i>European Union</i> ^[n 1]	18,769,286
2	 China ^[n 2]	13,457,267
3	 Japan	5,070,626
4	 Germany	4,029,140
5	 United Kingdom	2,808,899
6	 France	2,794,696
7	 India	2,689,992
8	 Italy	2,086,911
9	 Brazil	1,909,386
10	 Canada	1,733,706
11	 South Korea	1,655,608
12	 Russia ^[n 3]	1,576,488
13	 Spain	1,437,047
14	 Australia	1,427,767
15	 Mexico	1,199,264
16	 Indonesia	1,005,268
17	 Netherlands	909,887
18	 Saudi Arabia	769,878
19	 Turkey	713,513
20	 Switzerland	709,118
21	 Taiwan	602,678
22	 Sweden	554,659

Republic of
Cybercrime*

US \$608 Billion

*Not a real country



Bad Guys

Good Guys

CAREER POSSIBILITIES

2.93

Million



45.6

Thousand





The New York Times

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017



1031

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

Equifax shares slump on disappointing third-quarter earnings

Published: Oct 24, 2018 4:53 p.m. ET



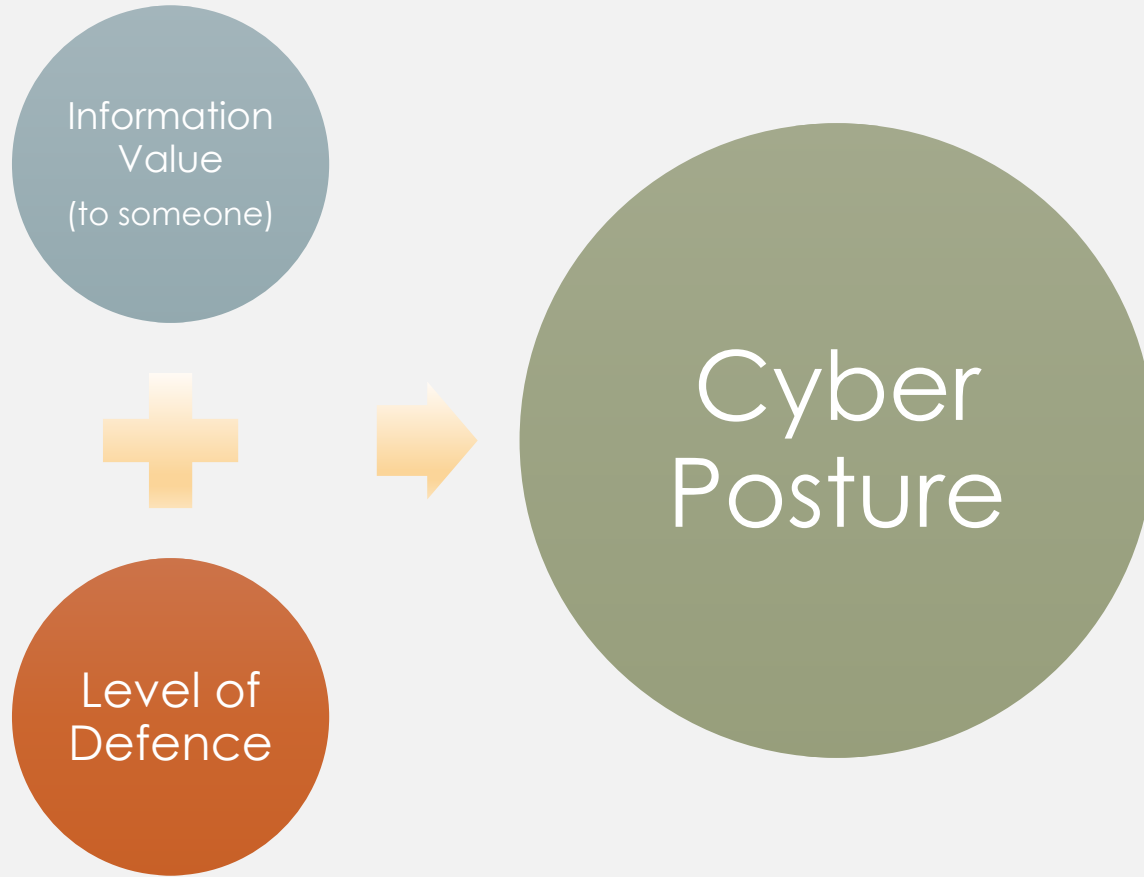
Aa



By
**SUE
CHANG**
MARKETS REPORTER



Shares of Equifax Inc. **EFX**, -1.14% skidded in Wednesday's extended session after the credit reporting agency missed both quarterly profit and revenue targets. Equifax reported its third-quarter earnings sank to \$38.4 million, or 32 cents a share, from \$96.3 million, or 79 cents a share, a year earlier. On an adjusted basis, the company would have earned \$1.41 a share. Revenue fell fractionally to \$834.2 million from \$834.8 million. Analysts surveyed by FactSet had forecast earnings of \$1.42 a share on revenue of \$857 million. The company also revealed that it recorded expenses of \$116.5 million in the third quarter and \$221.5 million in the first nine months of this year related to the data breach incident last year. For the fourth quarter, the agency projected adjusted earnings per share of \$1.30 to \$1.35, below the average \$1.43 forecast by analysts. Equifax shares slid 10% after hours.





We need to buy a new firewall because our old one doesn't do IDS, its only got 4 ports and the pins on the console port have snapped.

Your organization needs the latest best-in-breed technology to enable it to digitize, innovate, be disruptive, be agile and protect itself from bad people.



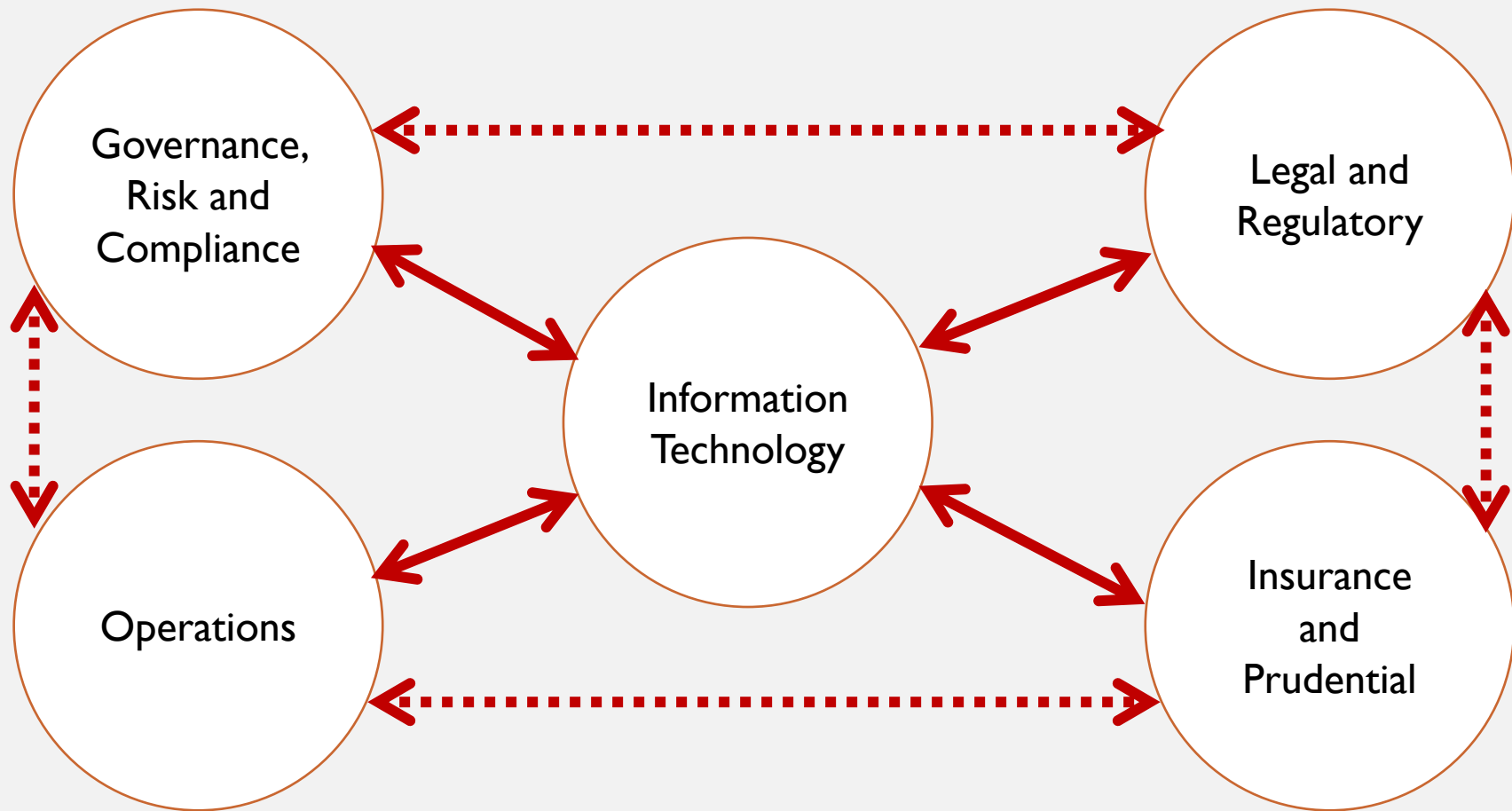
A man with dark hair, glasses, a checkered shirt, a purple tie, and suspenders is sitting at a desk. His hands are on a white keyboard. He has a serious expression. A yellow speech bubble tail points from his mouth towards the text on the right.

We need to update our cyber defenses.

If we don't, it presents a significant risk to our business.

If we get breached, the organization will be in all sorts of legal and financial mess.

Do you want to sleep at night?



CYBER LIFE LESSONS

- Even if you really are the smartest person in the room, don't act like you are.
- Calling someone “dumb” if they used “password” as their password or clicked on a phishing email won't do you any favours.
- Cyber people aren't exactly the life of the party, nor are we regarded as the charming types.
- Learn to speak business.

CYBER LIFE LESSONS

- Accept that not everyone cares about cyber security and IT. In fact, some people *hate* IT and think what they see on CSI is “cyber”.
- Cyber security is a life commitment. What you will learn now will probably be useless in 5-10 years. You will always keep learning about new technologies, attack vectors, scams etc.
- Cyber security is less “tech” and more psychology.

CYBER CAREER LESSONS

- Find a job that involves you using your brain.
- Push yourself into areas where you can leverage your skills and pursue your interests.
- Graduating won't be the end of your learning for your career, but rather your start.
- Consider cyber security from the perspective of the non-IT person. Is what you are saying engaging and interesting to them? No? Time to change your approach.
- An old firewall configured well is far more valuable than a state of the art firewall configured with ANY-ANY.

THANK YOU

Tony Vizza

<https://www.linkedin.com/in/tonyvizza/>