Cybersecurity information sharing (communication) state experience

Eng. Fahad Alanzi

Kuwait-DGCA

Introduction

state journey with respect to information sharing of cybersecurity attacks, vulnerabilities, and difficulties encountered by stakeholders. Aiming to mitigate attacks and vulnerabilities for speedy recovery and to prevent reoccurrence.

travel is complex industry that involves many entities, whom need to work collaboratively and collectively.

It is obvious that any attack on one stakeholder will harm the rest, hence; to achieve optimum result; they must work together, and the only way to do is through communication and information sharing.

Why communication critical !!!

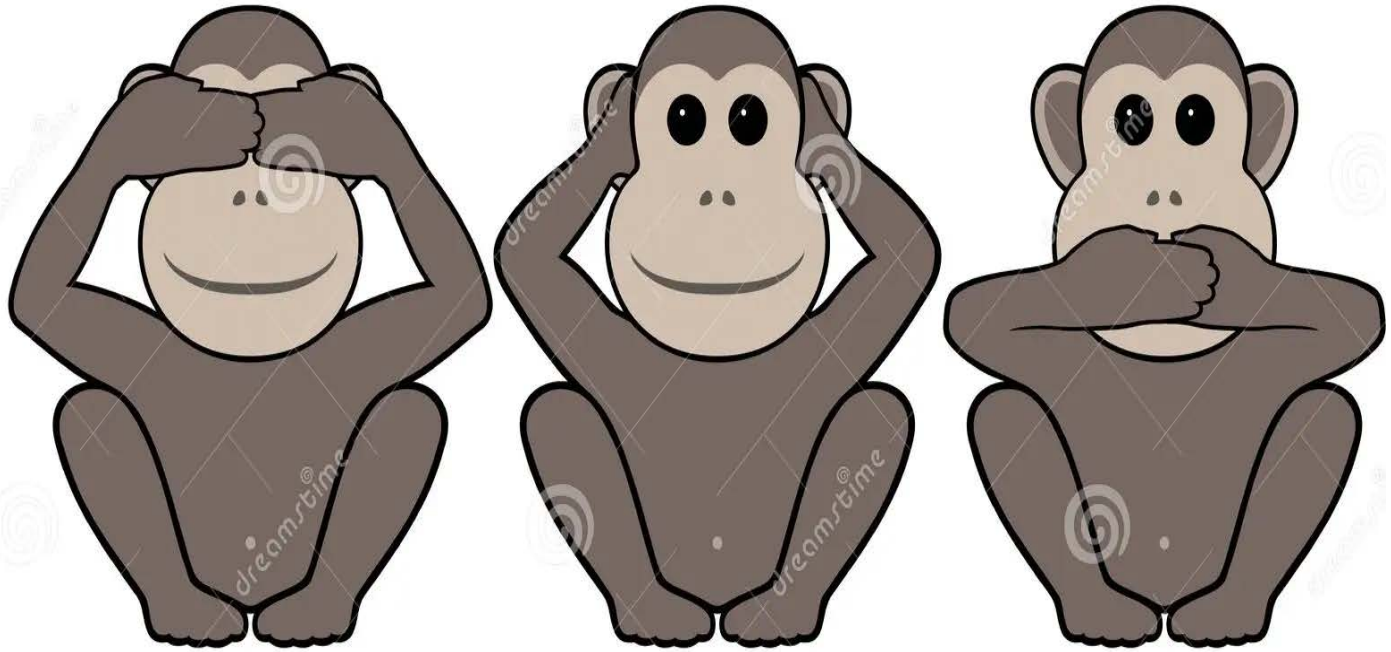
Starting from booking (tickets, accommodation, transport), through airport check in, passport control, screening, boarding an aeroplane that is equipped with latest data sharing like WIFI/Satellite, to arriving to another airport which nowadays utilises latest smart digital services. All of these services are offered by different entities (Authorities, airlines, security providers, ground handlers. Airport operators….) and in many cases same platforms. Like other access points These smart services became targets terrorists and malicious groups.

Cyber-attacks and vulnerabilities differ to traditional AVSEC breaches, they are discreet, not visible, and isolated. If not shared will stay in dark until they hit again.

For that it became obvious why national and international regulations request, encourage, and recommend Aviation community to communicate and have necessary mechanism to detect, deter, record, and recover to act as a shield against any attacks.

Challenges to flawless communication

- Cultural (shame, blame, old school)
- Resources (financial, allocating priorities)
- Know how.
- Outsourced services
- Lack of trust (consequences, reputation)



Overcoming Challenges

For a healthy communication and to establish communication between stakeholders; a trust bridge must be built which should be strong, discreet, worthy enough to allow flawless honest communication, and this can be done through:

- Meetings (committees, SOC)
- Relevant regulation (NPR, discreet)
- Mutual interest.
- Combined training.
- Campaign to raise awareness.

Our plan

DGCA drafted a plan to overcome these challenges and instil trust within stakeholders. To pave the way for a healthy communication cultural within the state/Airport, to exchange experiences, Information and ideas, This was accomplished at State level by working with CITRA, and at Airport level by :

- **Establishing Cybersecurity committee** where it's members from all stakeholders at Airport, to discuss all matters relating to Cybersecurity to minimize time of decision making and proper flow of information.
- **Circulating a Questioner** to all stakeholders to identify challenges and deficiencies that are existing and use this data as a tool to decide next course of action and efficient use of recourses.
- **continuous assessment** carried out by dedicated authority, to ensure that measures are developed to protect critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of air travel.

درجة المطلوب	درجة الامتثال			تاريخ التطبيق المتوقع	عوائق (مادية-بشرية-قانونية-إدارية)	الأدلة (وثائق-جداول-إجراءات-مراسلات)	الملاحظات
	نعم	لا	جزئي				
س1: هل يوجد لديكم إدارة او قسم مختص في الامن السيبراني (الشبكات والنظم)؟							
س2: هل يوجد لديكم برنامج أمني؟							
س3: هل يشمل برنامجكم الامني أمن الشبكات والنظم؟							
س4: هل لديكم برنامج وجدول تدريب لأمن الشبكات والنظم؟							
س5: هل يتم عقد دورات وعي أمني لجميع مستخدمي الأجهزة في كافة مجالات العمل؟							

درجة المطلوب	درجة الامتثال			تاريخ التطبيق المتوقع	عوائق (مادية-بشرية- قانونية-إدارية)	الأدلة (وثائق-جداول- إجراءات-مراسلات)	الملاحظات
	نعم	لا	جزئي				
س6: هل توجد برامج حماية ضد الهجمات؟ (anti-virus protection programs)							
س7: هل يتم تحديث برامج الحماية الأمنية في الشبكات والنظم؟							
س8: هل لديكم إجراءات مكتوبة لأمن الشبكات والنظم؟							

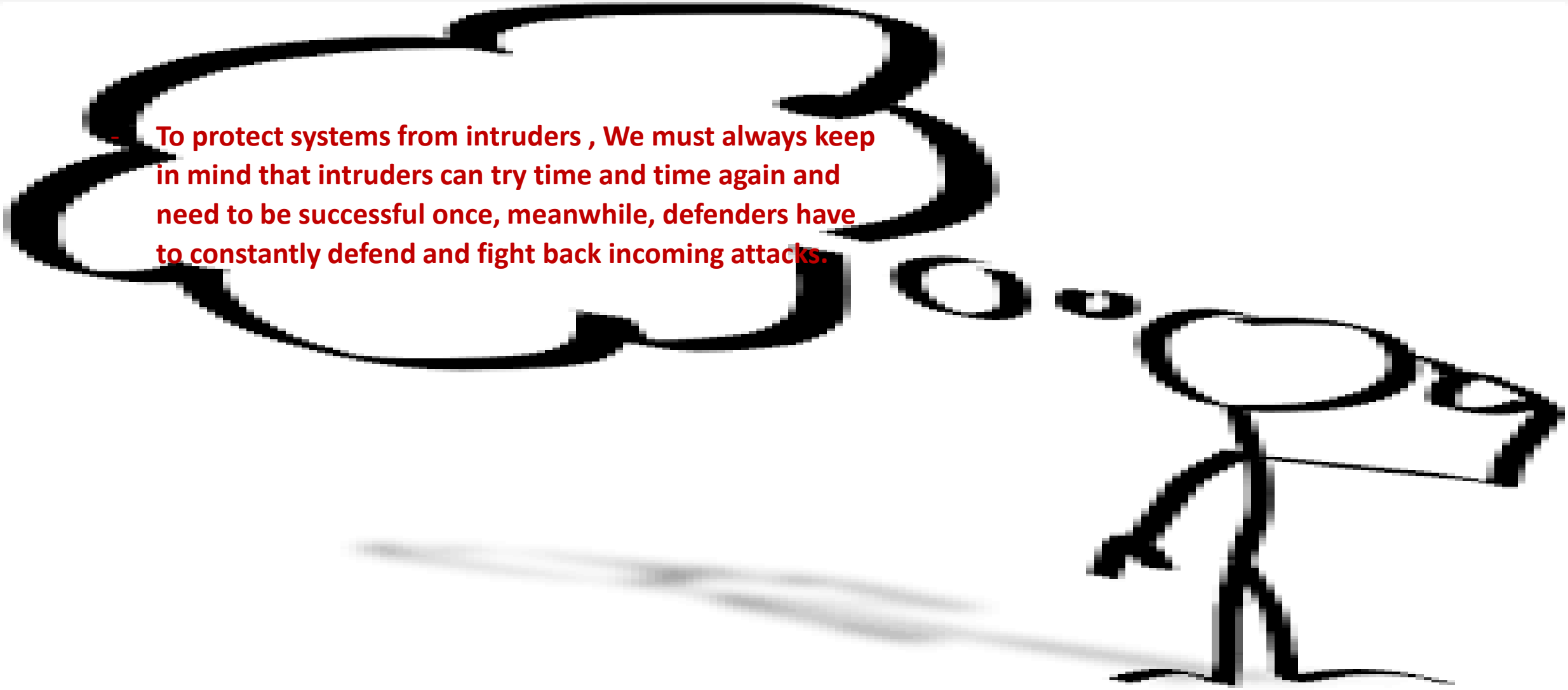
درجة المطلوب	درجة الامتثال			تاريخ التطبيق المتوقع	عوائق (مادية-بشرية- قانونية-إدارية)	الأدلة (وثائق-جداول- إجراءات-مراسلات)	الملاحظات
	نعم	لا	جزئي				
س9: هل يتم تطبيق إجراءات أمن الشبكات والنظم؟							
س10: هل يوجد ضمن إدارة المعلومات قسم او قدرة على تقييم المخاطر فيما يخص الامن السيبراني (الشبكات والنظم)؟							
س11: هل تم عمل تقييم سابق للمخاطر لأمن الشبكات والنظم للتعرف على نقاط الضعف؟							

درجة المطلوب	درجة الامتثال			تاريخ التطبيق المتوقع	عوائق (مادية-بشرية-قانونية-إدارية)	الأدلة (وثائق-جداول-إجراءات-مراسلات)	الملاحظات
	نعم	لا	جزئي				
س12: هل لديكم الأعداد الكافية من الطاقات البشرية من حيث العدد والتخصص لأمن الشبكات والنظم؟							
س13: هل تم تدريب موظفي الشبكات والنظم فيما يتعلق بأمن الشبكات والنظم؟							
س14: هل لديكم أرشيف على التهديدات المتعلقة بالشبكات والنظم؟							
س15: هل يتم إخطار السلطة المعنية (إدارة أمن الطيران المدني) في حال تعرض نظمكم لأي هجمات؟							

Conclusion

With increasing numbers of passengers, it's imperative that smart technology is the way forward .

Hence, Regulator , and all stakeholders must *communicate*, for effective cooperation to achieve a proactive approach against evolving technology threats.


To protect systems from intruders , We must always keep in mind that intruders can try time and time again and need to be successful once, meanwhile, defenders have to constantly defend and fight back incoming attacks.

THANK YOU