ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Εθνικό Πλαίσιο Κυβερνοασφάλειας

Γιώργος Δρίβας
Αν. Προϊστάμενος Τμήματος Ασφάλειας Πληροφοριών & Δικτύων
Διεύθυνση Κυβερνοασφάλειας
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Περιεχόμενα

- Κυβερνοασφάλεια σε ΕΕ και Ελλάδα
- Εθνικό Πλαίσιο Κυβερνοασφάλειας (ΕΠΚ)
  - Αναγκαιότητα
  - Δομή
  - Στόχοι ΕΠΚ
  - Περιγραφική προσέγγιση του ΕΠΚ
- Ο ρόλος της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ)
  - Στρατηγικές & Εργαλεία εφαρμογής
  - Μέθοδοι υλοποίησης
- Η Υπουργική Απόφαση 1027/8-10-2019
- Επόμενες ενέργειες / Άμεσες προτεραιότητες
- Εθνική Στρατηγική Κυβερνοασφάλειας

Η εξέλιξη της ασφάλειας των ΤΠΕ

- Νέα πεδία/εξελίξεις
  - IoT
  - Blockchain
  - AI
  - 4th Industrial Revolution

- Η ασφάλεια ως **βασικός πυλώνας** του Ψηφιακού μετασχηματισμού

→ Από την προαιρετικότητα στην **αναγκαιότητα**

Στην Ευρώπη…

- Η Ευρώπη εκπροσωπεί το **26%** της παγκόσμιας αγοράς κυβερνοασφάλειας
- Το **30%** της Ευρωπαϊκής ζήτησης καλύπτεται από εταιρείες εκτός ΕΕ
- Η Ευρώπη αποτελεί έδρα μόνο για το **14%** από τις 500 μεγαλύτερους παρόχους υπηρεσιών Κυβερνοασφάλειας

Στην Ευρώπη…

- Εργασίες Εφαρμογής της Οδηγίας NIS
  - Επιτελική Ομάδα **Cooperation Group**
  - Ομάδες ειδικών εργασιών – **Horizontal Working Group**
    - Hybrid Threats
    - 5G Risk Assessment
    - Cross border dependencies
    - E-elections
    - …

- Νέες διευρυμένες αρμοδιότητες για **ENISA**
- Νέος ρόλος για **πιστοποίηση προϊόντων** ασφάλειας ΤΠΕ
- Νέος φορέας για PPP (**ECSO - 2016**)
- Νέος φορέας για εκπαίδευση cyber ETEE platform (**ESDC - 09/2018**)
- Νέος φορέας για R&D (**European Cybersecurity Research and Competence Centre - TBA**)

→ **Τάση για ενοποίηση της αντιμετώπισης** των απειλών στον Κυβερνοχώρο σε πολλαπλά επίπεδα (Διπλωματικό, Στρατιωτικό, Εγκληματικές ενέργειες, Κρίσιμες Υποδομές, παροχή βασικών Υπηρεσιών, …)

…στην Ελλάδα

Ελλείψεις που αφορούν κυρίως σε:

- **Ανάπτυξη ικανοτήτων**
  - Καλές πρακτικές κυβερνοασφάλειας
  - Ερευνητικά προγράμματα
  - Εκπαιδευτικά προγράμματα
  - Μηχανισμοί κινήτρων
- **Συνεργασίες**
  - Συνεργασία μεταξύ υπηρεσιών
  - Συνεργασία δημοσίου-ιδιωτικού τομέα
  - Διμερείς συμφωνίες

…στην Ελλάδα

- **Έλλειψη εξειδικευμένου προσωπικού (+Brain drain)**
  - **→Κίνητρα παραμονής**
  - Τόνωση της εγχώριας έρευνας & ανάπτυξης
  - Απορρόφηση Ευρωπαϊκών προγραμμάτων
    - CEF ~10 mln
    - Digital Europe 2/9,2 bln
  - Τόνωση της εγχώριας αγοράς μέσω υποχρεωτικότητας μέτρων ασφάλειας στα έργα ΤΠΕ
    - Security by default & by design
    - SDLC Security

Εθνικό Πλαίσιο Κυβερνοασφάλειας (ΕΠΚ)

…**ως ένα σύνολο** ρόλων, συσχετισμών και κανόνων διαλειτουργικότητας μεταξύ των εμπλεκομένων φορέων

…**ως απαραίτητο εργαλείο** εφαρμογής της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Χαρακτηριστικά:

- Ταχύτητα & ευελιξία
- Οικονομικά αποδοτικό (Cost efficiency)
- Εξωστρέφεια & Συνεργατικότητα

Εξειδίκευση ΕΠΚ

Γιατί;
Τι;
Ποιός;
Πώς;

Δομικά στοιχεία ΕΠΚ

- **Άνθρωποι**
  - Εκπαιδεύσεις
  - Συνέργειες
  - Χρήση μητρώων συνεργατών
- **Διαδικασίες**
  - Κοινο πλαίσιο ασφάλειας
  - Εξειδικεύσεις ανά τομέα
  - Διεθνή πρότυπα και πρακτικές
- **Τεχνολογίες**
  - Τις παρέχει η αγορά
  - Τις αναπτύσσει η ακαδημαϊκή κοινότητα μέσω ερευνητικών προγραμμάτων

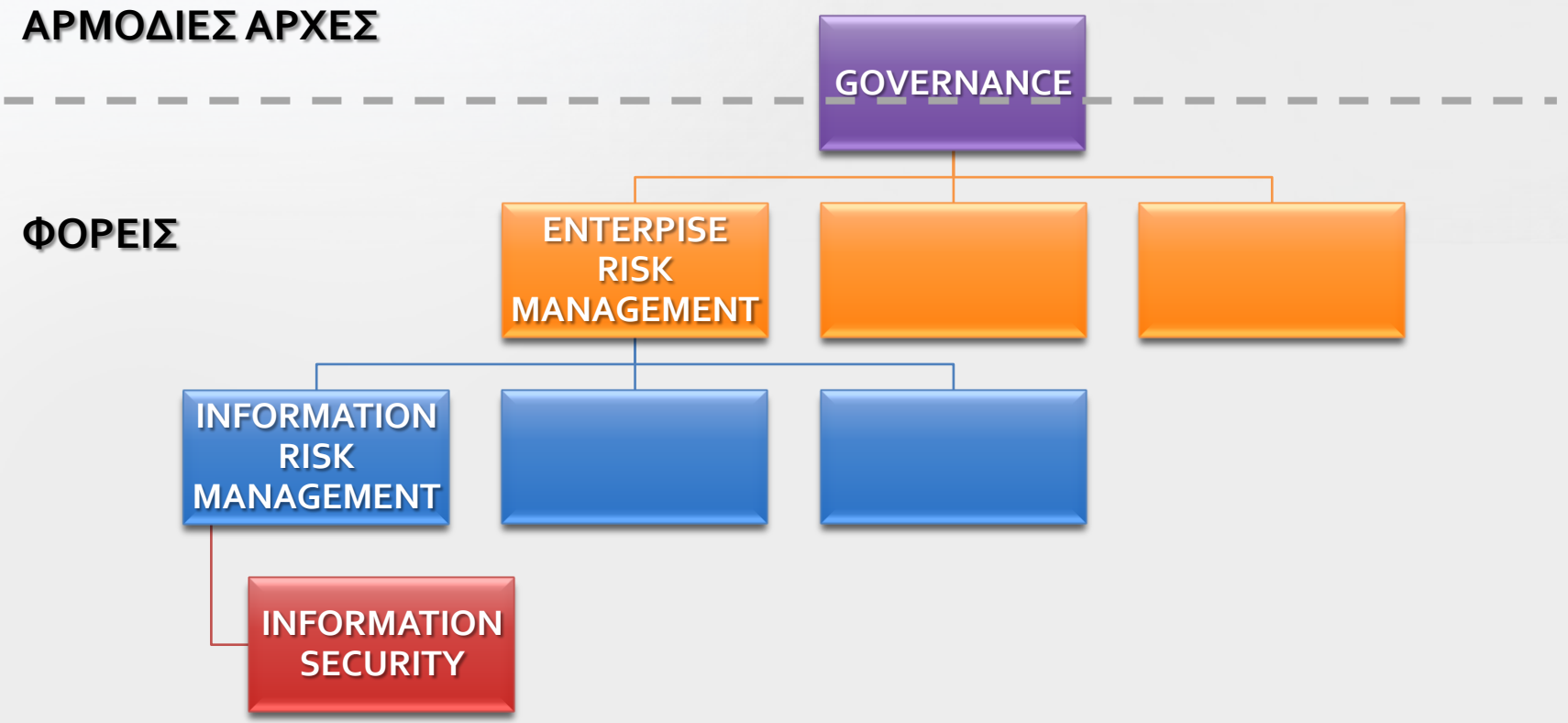
Εμπλεκόμενοι στην Κυβερνοασφάλεια

- **Στρατηγικό** – οι εμπλεκόμενοι φορείς υπό το συντονισμό των αρμόδιων εθνικών αρχών Κυβερνοασφάλειας
- **Επιχειρησιακό**
  - CERTs / CSIRTs
  - Δίωξη Ηλ. Εγκλήματος (ΕΛΑΣ)
  - Διεύθυνση Κυβερνοάμυνας (ΓΕΕΘΑ)

+ Τομεακές Ρυθμιστικές/Εποπτικές Αρχές (Υπουργεία, Ρυθμιστικές και Ανεξάρτητες Αρχές,…)
+ Ακαδημαϊκή κοινότητα
+ Πάροχοι Υπηρεσιών
+ Κοινότητες πολιτών

→ Όλοι όσοι κάνουν χρήση του Κυβερνοχώρου (…**ΟΛΟΙ**)

Συσχετισμοί Κυβερνοασφάλειας



Ο ρόλος της ΕΑΚ στην εφαρμογή του πλαισίου

Να **επέμβει** όπου και όταν

- Απαιτείται κεντρικός συντονισμός
- Υπάρχουν σοβαρά κενά (π.χ. νομοθετικά)

Να **λύσει** πιθανά αδιέξοδα της αγοράς

- Κόστος ανάπτυξης λύσεων
- Αποτυχία αυτορρύθμισης (Market irregularities & Failures)

Να **συνδέσει** τις ανάγκες της αγοράς με τις στρατηγικές κατευθύνσεις της χώρας

Να **προωθήσει** συνεργατικά μοντέλα και πρωτοβουλίες

Μεθοδολογία εφαρμογής του πλαισίου

- Να εντοπίσει τα προβλήματα
- Να αναγνωρίσει τα οριζόντια - επαναλαμβανόμενα
- Να αξιολογήσει τις πιθανές λύσεις
- Να προωθήσει τις πλέον αποτελεσματικές και αποδοτικές

Αρχές υλοποίησης

- Κανόνας του 80/20 (Αρχή Pareto) → προτεραιότητα σε **γρήγορες λύσεις με μεγάλο αντίκτυπο**
- Προσέγγιση **βάση κινδύνου** (Risk based / tailor fitted)
- Εφαρμογή **μοντέλου Ωριμότητας** (Επίπεδο 0-5)

Αρχές υλοποίησης

Εξέλιξη Επιπέδου Ωριμότητας

Στρατηγικές και εργαλεία εφαρμογής

- **Συνεργασίες** μεταξύ φορέων και συνέργειες δημοσίου-ιδιωτικού τομέα
- Αξιοποίηση **ευρωπαϊκών χρηματοδοτικών** εργαλείων (CEF, H2020, Digital Europe)
- **Ευέλικτη προσέγγιση** (Agile) κατά την εφαρμογή
- Αξιοποίηση **έτοιμων λύσεων** (υπάρχον φορείς και τεχνολογικές λύσεις)
- **Ανταλλαγή Γνώσης** με άλλες χώρες (π.χ. Φινλανδία, Εσθονία, Γερμανία, Γαλλία)

Κύκλος Ζωής ΕΠΚ

- **Σχεδιασμός** → ΕΑΚ με Ομάδες Εργασίας
- **Υλοποίηση** → Φορείς
- **Αξιολόγηση** → Υπό την επίβλεψη της ΕΑΚ
  → Εσωτερική (Αυτοαξιολόγηση)
  → Εξωτερική (Εξωτερική ανάθεση)
- **Διόρθωση/Επαναπροσδιορισμός** → Φορείς με καθοδήγηση της ΕΑΚ

Υπουργική Απόφαση (ΥΑ1027/8-10-2019)

- **Κριτήρια και κατάλογος ΦΕΒΥ**
  - 7 τομείς
  - Κατάλογος Βασικών Υπηρεσιών
  - ΦΕΒΥ 10% της αγοράς (πελάτες ή μερίδιο αγοράς)
- **Κρίσιμη Διατάραξη**
  - Χρήστες (> 50.000)
  - Χρηστοώρες (> 100.000)
  - Κόστος (> 1.000.000)
  - Απειλή ανθρώπινης ζωής
- **Διαδικασία κοινοποίησης περιστατικού**
  - Εντός 24 ωρών
  - Ιστοσελίδα αναφοράς περιστατικού

https://ncsa.mindigital.gr/

Υπουργική Απόφαση (ΥΑ1027/8-10-2019)

- **Έλεγχος και κυρώσεις**
  - Αναφορά αυτοαξιολόγησης ή/και έλεγχος
  - Σύσταση, επίπληξη, πρόστιμο (< 200.000€)

Ενιαία Πολιτική Ασφάλειας

Τήρηση ενός **ενιαίου ελάχιστου βασικού επιπέδου ασφάλειας** των συστημάτων δικτύου και πληροφοριών
→ εφαρμογή **Ενιαίας Πολιτικής Ασφάλειας**.

Κάθε φορέας θεσπίζει, υλοποιεί και διατηρεί επίκαιρη **Πολιτική Ασφαλείας** σχετική με την ασφάλεια των συστημάτων δικτύου και πληροφοριών, **η οποία καλύπτει τουλάχιστον όσα ορίζει η Ενιαία Πολιτική Ασφάλειας**.

Η Πολιτική Ασφάλειας, μεταξύ άλλων:

- ορίζει **Στρατηγικούς Στόχους**
- περιγράφει τη **Διακυβέρνηση**
- παραπέμπει σε άλλες **Συμπληρωματικές Πολιτικές**

Ενιαία Πολιτική Ασφάλειας

Βασικοί στόχοι να διασφαλίσει ο φορέας:

- την **εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα** των δεδομένων έναντι εκούσιων ή ακούσιων απειλών
- την ικανοποίηση των σχετικών **νομικών και ρυθμιστικών απαιτήσεων** σχετικών με την ασφάλεια και προστασία δεδομένων
- την **επιχειρησιακή συνέχεια** των βασικών υπηρεσιών του φορέα έναντι περιστατικών κυβερνοεπιθέσεων
- την **ενημέρωση και την εκπαίδευση** όλων των υπαλλήλων και εμπλεκομένων τρίτων σχετικά με την παροχή των βασικών υπηρεσιών του φορέα
- την άμεση **κοινοποίηση και διαχείριση περιστατικών** ή αδυναμιών ασφαλείας

Ενιαία Πολιτική Ασφάλειας

Αρμόδιοι:

- η **Διοίκηση** του φορέα, η οποία **εγκρίνει, αναθεωρεί και είναι αρμόδια** για την αποτελεσματική και αποδοτική εφαρμογή της Πολιτικής Ασφάλειας.

- ο **Υπεύθυνος Ασφάλειας Πληροφοριών**, ο οποίος **επιβλέπει και συντονίζει** την εφαρμογή αυτής της πολιτικής μέσω χρήσης κατάλληλων προτύπων, διαδικασιών και διεθνών πρακτικών και λειτουργεί ως **σημείο επαφής** με τους αρμόδιους φορείς.

- όλο το **προσωπικό** και οι συμβεβλημένοι **προμηθευτές**, οι οποίοι **ακολουθούν τις διαδικασίες** για την τήρηση της πολιτικής ασφάλειας πληροφοριών.

→ Η Πολιτική Ασφαλείας θα πρέπει να λαμβάνει μέριμνα για την τήρηση των **"Βασικών Απαιτήσεων Ασφάλειας"**, όπως αυτές ισχύουν και ορίζονται από την Εθνική Αρχή Κυβερνοασφάλειας.

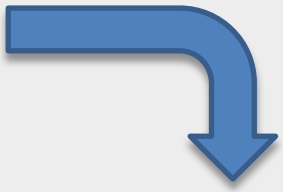
Βασικές Απαιτήσεις Ασφάλειας

1. Επιχειρησιακό περιβάλλον
2. Διαχείριση πόρων
3. Αποτίμηση επικινδυνότητας
4. Στρατηγική διαχείρισης κινδύνων
5. Διαχείριση κινδύνων αλυσίδας εφοδιασμού
6. Αυτοαξιολόγηση – Βελτίωση
7. Πολιτικές, διεργασίες και διαδικασίες προστασίας βασικών υπηρεσιών
8. Διαχείριση ταυτότητας και έλεγχος πρόσβασης
9. Φυσική και περιβαλλοντική ασφάλεια
10. Ασφάλεια συστημάτων και εφαρμογών
11. Ασφάλεια δεδομένων
12. Αντίγραφα ασφαλείας
13. Τεχνολογίες ασφάλειας
14. Δοκιμές συστημάτων
15. Διαχείριση Αλλαγών
16. Ευαισθητοποίηση και κατάρτιση
17. Ανίχνευση απειλών
18. Διαχείριση Περιστατικών
19. Επιχειρησιακή συνέχεια
20. Ανάκαμψη από καταστροφές

Επιλογή Μέτρων Ασφάλειας

- Ενθαρρύνεται η χρήση **διεθνώς αποδεκτών προτύπων, προδιαγραφών και οδηγών** που σχετίζονται με την ασφάλεια των συστημάτων δικτύων και πληροφοριών.
  - ISO
  - NIST
  - ISACA
  - OWASP

→ όποιο ταιριάζει καλύτερα στις **ειδικές ανάγκες** του φορέα (…**αρκεί να πληρούνται τα κάτωθι**)



Επιλογή Μέτρων Ασφάλειας

Θα πρέπει να λαμβάνουν μέριμνα ώστε αυτά να είναι:

- **Αποτελεσματικά**, ώστε να αυξάνουν το επίπεδο ετοιμότητας του φορέα έναντι τωρινών και μελλοντικών απειλών ασφάλειας.
- **Αποδοτικά**, ώστε να επιλέγονται αυτά τα οποία θα έχουν το μεγαλύτερο αντίκτυπο στην ενίσχυση της ασφάλειας ενός φορέα, σε σχέση με τις απαιτήσεις κτήσης και διατήρησης.
- **Κατάλληλα**, ώστε να είναι συμβατά και να διευκολύνουν τη παροχή των βασικών υπηρεσιών του φορέα.
- **Αναλογικά**, ώστε να επιλέγονται συναρτήσει του εκάστοτε επιπέδου επικινδυνότητας.
- **Συγκεκριμένα**, ώστε να διασφαλίζεται ότι τα μέτρα θα εφαρμόζονται στην πράξη και θα ενισχύουν ενεργά το επίπεδο ασφάλειας.
- **Αξιόπιστα**, ώστε να παρέχουν δείκτες και αποδείξεις για την αποτελεσματική και αποδοτική εφαρμογή τους.
- **Περιεκτικά**, ώστε η εφαρμογή τους να καλύπτει όσες περισσότερες βασικές απαιτήσεις ασφάλειας είναι δυνατό.

Πλαίσιο Αυτοαξιολόγησης Ωριμότητας

- «Βασικές Απαιτήσεις Ασφάλειας»
  → **20 σημεία αξιολόγησης**
  →**Οδηγός Αξιολόγησης**

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Υπεύθυνος Ασφάλειας Πληροφοριών & Δικτύων

Ρόλος

- **Σημείο επαφής** και συνεργασίας με τις Αρμόδιες Αρχές
- Συντονίζει και επιβλέπει το Φορέα για **υποχρεώσεις που απορρέουν από διατάξεις** για θέματα Κυβερνοασφάλειας
- Εποπτεύει
  - την υλοποίηση της **πολιτικής** και των **απαιτήσεων ασφάλειας**
  - την **εκπαίδευση και ευαισθητοποίηση** του Φορέα σε θέματα Κυβερνοασφάλειας
  - Τη σύνταξη **αναφοράς αυτοαξιολόγησης** του φορέα

Προσόντα

- Να διαθέτει **σχετικές σπουδές** και **πιστοποιημένες γνώσεις**
- Να διαθέτει **εμπειρογνωσία** στον τομέα της ασφάλειας πληροφοριών και δικτύων (>5 ετών)
- Να γνωρίζει τις **επιχειρησιακές λειτουργίες** του Φορέα

Δίκτυο Υπευθύνων Ασφάλειας

- Δίκτυο συνεργασίας
  - Καθολική Συμμετοχή με σταδιακή διεύρυνση
  - Τακτικές συναντήσεις
  - Ειδικές ομάδες εργασίας

- Αρχικά σε επίπεδο Υπουργείων, όπου:
  - Τίθενται προβληματισμοί
  - Αναζητούνται διαθέσιμες λύσεις
  - Λαμβάνονται αποφάσεις από κοινού

→ **Μοντέλο Αποκεντρωμένης υλοποίησης με κεντρικό συντονισμό**

Στόχοι Εθνικού Πλαισίου Κυβερνοασφάλειας

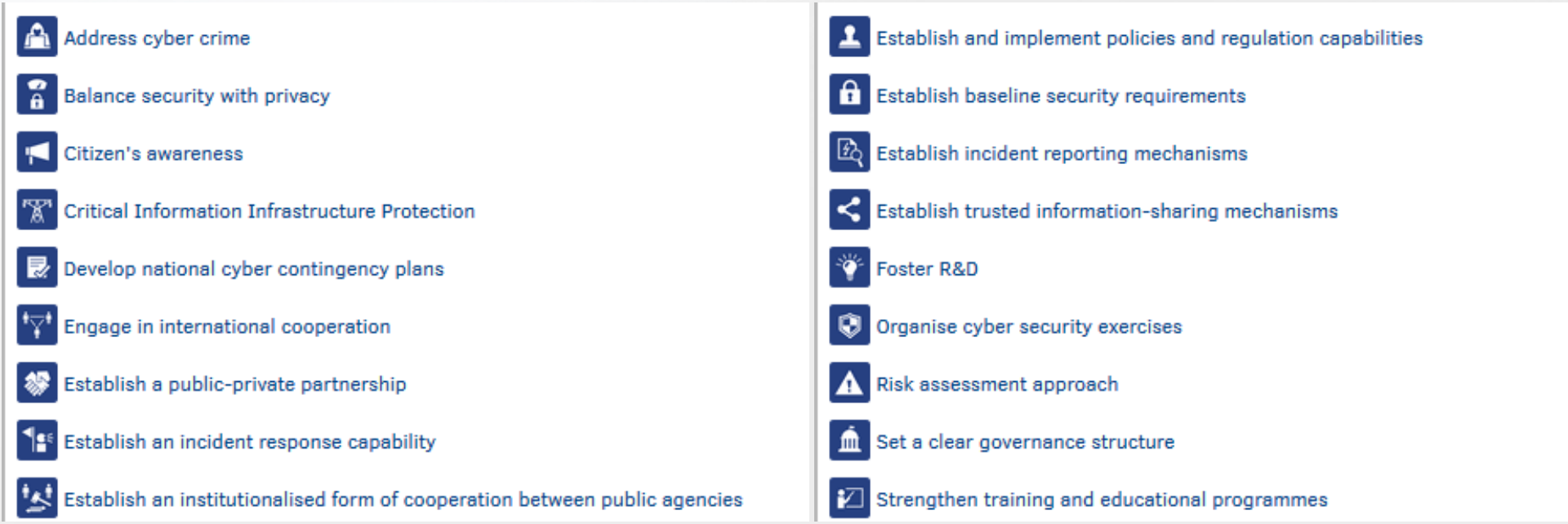
- Να βελτιωθεί άμεσα η θέση της χώρας στους **διεθνείς δείκτες**
- Να βελτιωθεί το επίπεδο ασφάλειας σε **πραγματικό** επίπεδο
- Να προαχθεί ο **ψηφιακός μετασχηματισμός** μέσα σε ένα κλίμα εμπιστοσύνης

Επόμενες ενέργειες / Προτεραιότητες

- Η συγκρότηση και ενεργοποίηση του **Δικτύου Υπευθύνων Ασφαλείας**
- Η επέκταση του Πλαισίου και στο **Δημόσιο τομέα**
- Κατάρτιση **Σχεδίου εκτάκτου ανάγκης** για απειλές στον Κυβερνοχώρο
- **Αποτίμηση Επικινδυνότητας** σε Εθνικό Επίπεδο

Εθνική Στρατηγική Κυβερνοασφάλειας

- Καλύπτει 18/20 προτεινόμενους στόχους του ENISA



→ Η πιο περιεκτική στρατηγική στην Ευρώπη σύμφωνα με την τελευταία αξιολόγηση του ENISA (09/2019)

Εθνική Στρατηγική - Πλαίσιο Δράσεων

1. Ορισμός των Φορέων που συμμετέχουν στην Εθνική Στρατηγική Κυβερνοασφάλειας
2. Ορισμός των Κρίσιμων Υποδομών
3. Αποτίμηση Επικινδυνότητας σε Εθνικό Επίπεδο
4. Καταγραφή και βελτίωση Υφιστάμενου Θεσμικού Πλαισίου
5. Εθνικό Σχέδιο Έκτακτης Ανάγκης στον Κυβερνοχώρο
6. Καθορισμός Βασικών Απαιτήσεων Ασφάλειας
7. Αντιμετώπιση Περιστατικών Ασφάλειας
8. Εθνικές Ασκήσεις Ετοιμότητας
9. Ευαισθητοποίηση χρηστών – πολιτών
10. Μηχανισμοί Αξιόπιστης Ανταλλαγής Πληροφοριών

11α. Υποστήριξη Ερευνητικών και Αναπτυξιακών Προγραμμάτων

11β. Υποστήριξη Ακαδημαϊκών Προγραμμάτων Εκπαίδευσης

12. Συνεργασίες σε Διεθνές Επίπεδο

NCSI National Cyber Security Index

RANKING METHODOLOGY ABOUT US

Greece 1st among 134 countries (14/10/2019) !

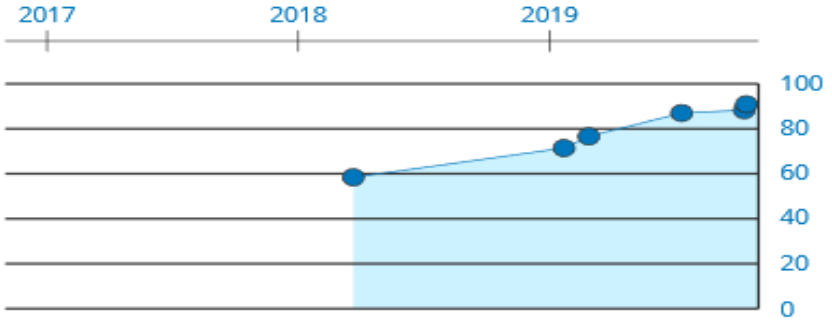
Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Greece	90.91	65.44	25.47
2.	Czech Republic	90.91	69.37	21.54
3.	Estonia	90.91	79.27	11.64

1. Greece 90.91

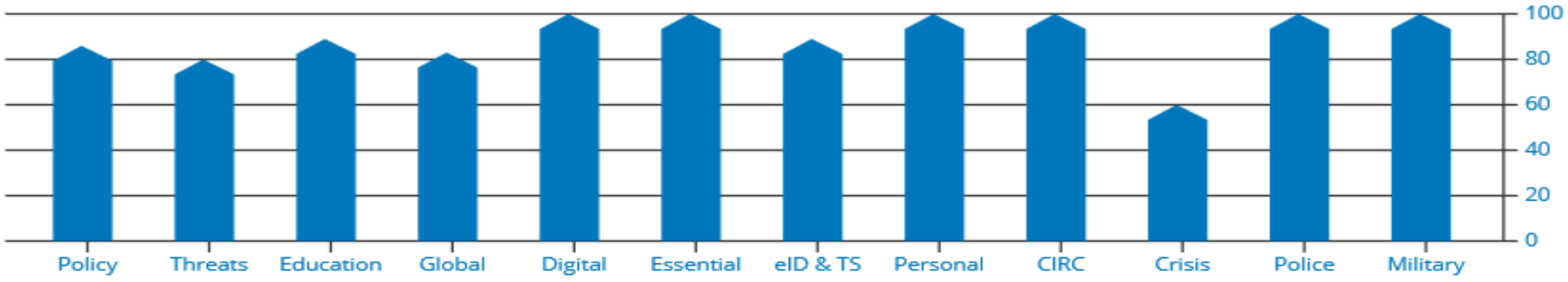
Population	10.9 million
Area (km²)	132.0 thousand
GDP per capita ($)	29.1 thousand

1st	National Cyber Security Index	91 %
77th	Global Cybersecurity Index	53 %
38th	ICT Development Index	72 %
70th	Networked Readiness Index	59 %

NCSI DEVELOPMENT TIMELINE



NCSI FULFILMENT PERCENTAGE



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Υπουργείο Ψηφιακής Διακυβέρνησης

Ευχαριστούμε!

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ncsa@mindigital.gr