



Selecting Essential IT Security Projects

Dimitris Gritzalis

July 2003

Κομβικά Έργα Ασφάλειας Πληροφοριών και Υποδομών

Δημήτρης Γκρίτζαλης (dgrit@aub.gr)

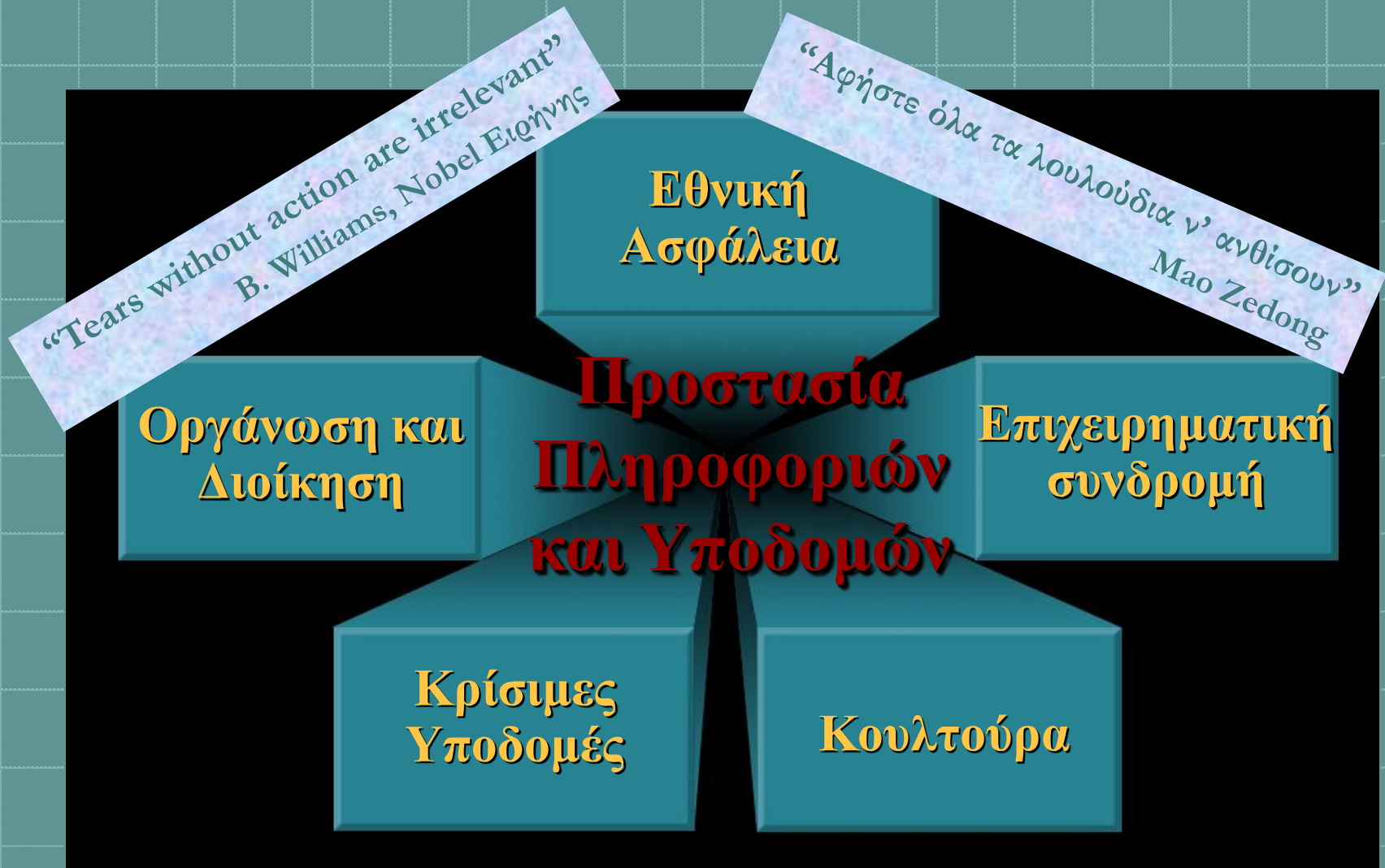
Αναπληρωτής Καθηγητής Ασφάλειας στην Πληροφορική και τις Επικοινωνίες
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Η παρουσίαση βασίζεται στη μελέτη **Ενσωμάτωση Λειτουργιών Ασφάλειας και Ιδιωτικότητας σε Πληροφοριακά Συστήματα και Εγκαταστάσεις**, η οποία χρηματοδοτήθηκε από την **Κοινωνία της Πληροφορίας ΑΕ** (Γενάρης 2003).

Κοινωνία της Πληροφορίας και Παγκοσμιοποίηση



Διαπλοκή και αλληλεπίδραση



Ασφάλεια Πληροφοριών

Ασφάλεια Πληροφοριών είναι η προστασία και τήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους (ISO/IEC 17799:2000)

Οπου:

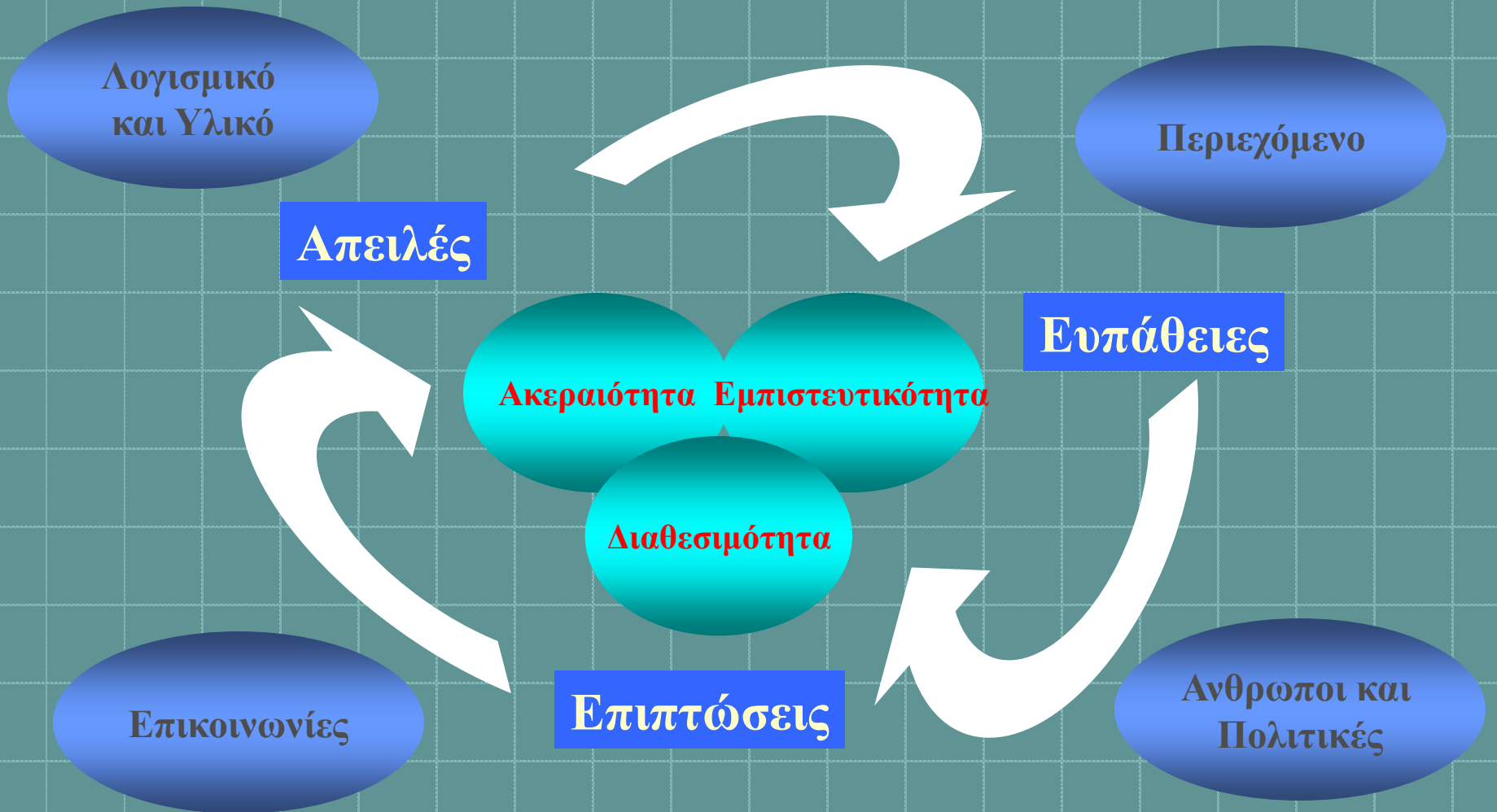
Εμπιστευτικότητα (**C**onfidentiality) είναι η διασφάλιση της προσπέλασης της πληροφορίας μόνο από εξουσιοδοτημένους χρήστες.

Ακεραιότητα (**I**ntegrity) είναι η διασφάλιση της ακρίβειας και πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας της.

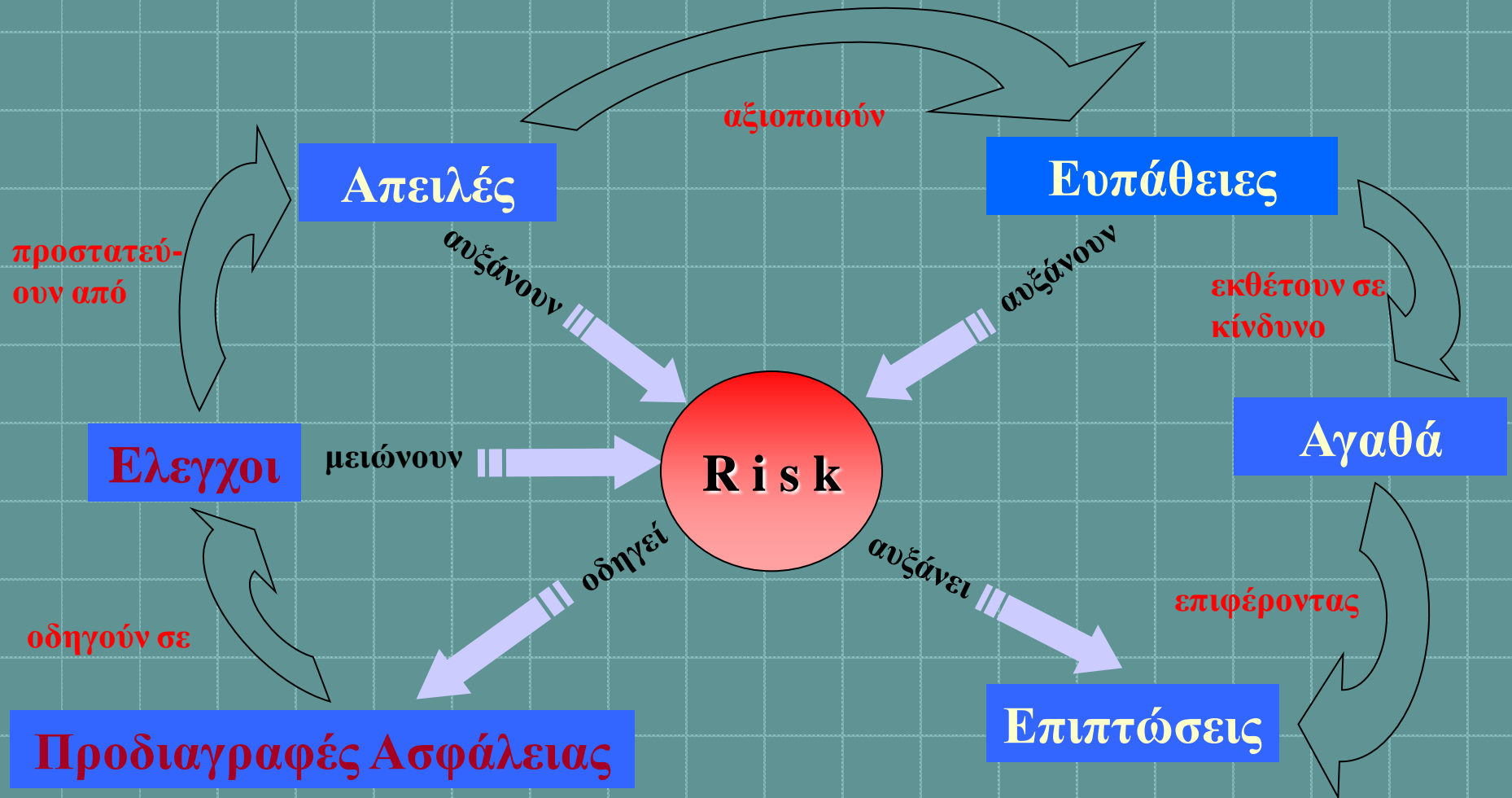
Διαθεσιμότητα (**A**vailability) είναι η διασφάλιση της προσπέλασης της πληροφορίας, από εξουσιοδοτημένους χρήστες, στον εύλογα προσδοκώμενο χρόνο.



Συνύπαρξη και διαπλοκή παραγόντων



Η κομβική έννοια της επικινδυνότητας (risk)



Προστασία Κρίσιμων Υποδομών

Προστασία κρίσιμων υποδομών είναι η προστασία των οργανισμών, δικτύων πληροφοριών και επικοινωνιών και δικτύων διανομής, τα οποία διασφαλίζουν τη διαρκή διανομή των αγαθών και των υπηρεσιών που είναι απαραίτητες για την εθνική άμυνα, οικονομία, δημόσια υγεία και ευμάρεια και ασφάλεια των πολιτών.

Τομείς: Γεωργία, Διατροφή, Υδρευση, Δημόσια Υγεία, Επείγουσες Υπηρεσίες, Δημόσια Διοίκηση, Εθνική Άμυνα, Πληροφορική, Ενέργεια, Μεταφορές, Επικοινωνίες, Χρηματοοικονομικά, Χημική Βιομηχανία, Ταχυδρομεία.

Πεδίο αναφοράς: **Κυβερνοχώρος.**



Παράδειγμα Οργάνωσης της Προστασίας Κρίσιμων Υποδομών



Κομβικοί τομείς παρέμβασης για την Ασφάλεια Πληροφοριών και Υποδομών



Κομβικά έργα Ασφάλειας Πληροφοριών και Υποδομών

Σχετική επιρροή του έργου στο σύνολο της παρέμβασης

1. Αποτίμηση Επικινδυνότητας και Πολιτική Ασφάλειας

2α. Μέτρα Ασφάλειας

2β. Προστασία Προσωπικών Δεδομένων

3α. Σχέδιο Συνέχισης Δραστηριοτήτων

3β. Σχέδιο Αντιμετώπισης Περιστατικών

3γ. Σχέδιο Ανάκαμψης από Καταστροφή

4. Πιστοποίηση Ασφάλειας

Αποτίμηση Επικινδυνότητας και Πολιτική Ασφάλειας (Risk Assessment and Security Policy)

- ✓ **Πρωταρχικό έργο** ασφάλειας για κάθε ΠΣ ή εγκατάσταση.
- ✓ **Αποτιμά** την επικινδυνότητα ενός ΠΣ ή μιας εγκατάστασης, με βάση τις αδυναμίες και τις ευπάθειές τους, καθώς και τις επιπτώσεις και τις συνέπειες που θα υποστούν από ένα περιστατικό ανασφάλειας.
- ✓ Περιγράφει τα **τεχνικά και οργανωτικά** μέτρα που είναι αναγκαία για την επαρκή ασφάλεια του ΠΣ ή της εγκατάστασης.
- ✓ Παρέχει ένα επεξεργασμένο **προσχέδιο πολιτικής ασφάλειας** ενός ΠΣ ή μιας εγκατάστασης.
- ✓ Είναι **υποχρεωτική από το νόμο**, τουλάχιστον για την επεξεργασία ευαίσθητων δεδομένων.



(Τεχνικά) Μέτρα Ασφάλειας

- ⊕ **Αναγκαία συμπλήρωση** της αποτίμησης επικινδυνότητας.
- ⊕ **Υλοποιεί** τα τεχνικά μέτρα ασφάλειας που υποδείχθηκαν από την αποτίμηση επικινδυνότητας.
- ⊕ **Διασυνδέει** τα τεχνικά μέτρα ασφάλειας με τα οργανωτικά μέτρα ασφάλειας τα οποία υλοποιεί ο κάτοχος του ΠΣ ή της εγκατάστασης.
- ⊕ **Επιδεικνύει** την αποτελεσματικότητα και την ορθότητα των μέτρων αυτών.
- ⊕ Για λόγους αξιοπιστίας, αλλά και δεοντολογίας, ο υλοποιητής των τεχνικών μέτρων ασφάλειας δεν πρέπει να είναι ο ίδιος με τον αποτιμητή επικινδυνότητας.



Προστασία Προσωπικών Δεδομένων και Ιδιωτικότητα (Personal Data Protection and Privacy)

- + Ειδικό έργο για την προάσπιση της ιδιωτικότητας και την καλλιέργεια μιας γόνιμης “**παιδείας ασφάλειας**” (security culture).
- + Αφορά ειδικά και μόνον τα ΠΣ που επεξεργάζονται **προσωπικά δεδομένα**.
- + Εντοπίζει τις παρεμβάσεις που είναι **αναγκαίες** για την προσαρμογή της λειτουργίας του ΠΣ (και της εγκατάστασης) στις απαιτήσεις των Νόμων 2472/97 και 2774/99.
- + **Περιγράφει** τη διαδικασία βηματικής προσαρμογής του ΠΣ ή της εγκατάστασης στις απαιτήσεις των ως άνω νόμων.
- + **Υλοποιεί** ορισμένα τμήματα της προσαρμογής αυτής.



Σχέδιο Συνέχισης Δραστηριοτήτων (Business Continuity Plan, BCP)

- ✚ **Υποδεικνύει** τις ενέργειες που πρέπει να γίνουν για τη συνέχιση της λειτουργίας ενός ΠΣ ή μιας εγκατάστασης, μετά από μια σημαντική ζημιά ή καταστροφή.
- ✚ **Περιλαμβάνει** ενέργειες προετοιμασίας και εφαρμογής των αναγκαίων διαδικασιών, με βάση προκαθορισμένους στόχους, οργανωτικά σχήματα, προμήθειες εξοπλισμού, συμφωνίες χρήσης εναλλακτικών πόρων κλπ.
- ✚ Θα μπορούσε να θεωρηθεί ως **υπερσύνολο** όλων των έργων ασφάλειας, αλλά τότε θα γινόταν πολύπλοκο και δαπανηρό, άρα μη ελκυστικό για τη μέση διοίκηση.



Σχέδιο Αντιμετώπισης Περιστατικών (Incident Handling)

- Ⓢ **Αποτιμά** τις συνέπειες που μπορεί να έχει στο ΠΣ ή στην εγκατάσταση ένα έκτακτο ανεπιθύμητο περιστατικό ή ένα απρόοπτο συμβάν, μη καταστροφικού χαρακτήρα.
- Ⓢ **Υποδεικνύει** συστηματικά τις ενέργειες που πρέπει να γίνουν για την αντιμετώπιση τέτοιων περιστατικών.
- Ⓢ **Αναφέρεται** σε προετοιμασία υποδομών, διαδικασιών, προμήθεια ειδικού εξοπλισμού, καθώς και σε θέσπιση σχετικών συμφωνιών.
- Ⓢ **Προτείνει** το οργανωτικό σχήμα που είναι απαραίτητο για την εφαρμογή του σχεδίου και για την αποτύπωση και μελέτη των σχετικών περιστατικών.



Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery)

- ❖ **Αποτιμά** τις συνέπειες που μπορεί να έχει στο ΠΣ ή στην εγκατάσταση ένα ενδεχόμενο μείζον-καταστρεπτικό συμβάν.
- ❖ **Υποδεικνύει** συστηματικά τις ενέργειες που πρέπει να γίνουν για την αντιμετώπιση τέτοιων περιστατικών.
- ❖ **Αναφέρεται** σε προετοιμασία υποδομών, διαδικασιών, προμήθεια ειδικού εξοπλισμού, καθώς και σε θέσπιση σχετικών συμφωνιών.
- ❖ **Προτείνει** το οργανωτικό σχήμα που είναι απαραίτητο για την εφαρμογή του σχεδίου.



Πιστοποίηση Ασφάλειας (Security Certification)

- # Αποτελεί έργο **τεχνικο-οργανωτικής ωριμότητας** και συνίσταται προς εφαρμογή κυρίως σε ΠΣ ή εγκαταστάσεις που (πρέπει να) παρέχουν επαρκή ή υψηλή ασφάλεια.
- # **Επιβεβαιώνει** ότι ένα ΠΣ ή μια εγκατάσταση πληροί τις προϋποθέσεις που θέτει ένα πρότυπο ασφάλειας.
- # Η **επιλογή** του προτύπου δεν είναι μονοσήμαντη, ενώ ενδέχεται να προκαλέσει μη αμελητέα οργανωτική-γραφειοκρατική όξυνση.
- # Ο ανάδοχος θα πρέπει να διαθέτει και ο ίδιος επαρκή εμπειρία και κατάλληλη **πιστοποίηση** και η αγορά να παρέχει λύσεις.



Συνοψίζοντας...

- Η ασφάλεια πληροφοριών και υποδομών μπορεί να στηριχθεί σε ορισμένα **κομβικά έργα**, εφόσον αυτά διασφαλίζουν συνεκτικότητα, ολοκληρωσιμότητα και διαλειτουργικότητα.
- Το σχέδιο δράσης που σκιαγραφήθηκε:
 - α) **Ικανοποιεί** τις προϋποθέσεις αυτές.
 - β) Είναι **συμβατό** με τις διαδικασίες προκήρυξης έργων ΤΠΕ.
 - γ) Προωθεί το **συγκερασμό** ασφάλειας και ιδιωτικότητας.
 - δ) Έχει ιδιαίτερα ελκυστικό δείκτη **κόστους-ωφέλειας**.
- Το σχέδιο δίνει απαντήσεις τόσο σε περιπτώσεις που υπάρχει σοβαρή **έλλειψη ασφάλειας**, όσο και σε παρεμβάσεις με **επείγοντα χαρακτήρα** και **στενά χρονικά περιθώρια** υλοποίησης.

References

1. Denault M., Gritzalis D., Karagiannis D., Spirakis P., "Intrusion detection: Evaluation and performance issues of the SECURENET system", *Computers & Security*, Vol. 13, No. 6, pp. 495-508, 1994.
2. Gritzalis D., *Secure Electronic Voting*, Springer, USA 2003.
3. Gritzalis D., "Principles and requirements for a secure e-voting system", *Computers & Security*, Vol. 21, No. 6, pp. 539-556, 2002.
4. Gritzalis D., "A baseline security policy for distributed healthcare information systems", *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
5. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
6. Gritzalis S., Iliadis J., Gritzalis D., Spinellis D., Katsikas S., "Developing secure web-based medical applications", *Medical Informatics*, Vol. 24, No. 1, pp. 75-90, 1999.
7. Gritzalis S., Gritzalis D., Moulinos K., Iliadis J., "An integrated architecture for deploying a virtual private medical network over the web", *Medical Informatics Journal*, Vol. 26, No.1, pp. 49-72, 2001.
8. Katsikas S., Spyrou T., Gritzalis D., Darzentas J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
9. Spinellis D., Gritzalis D., "PANOPTIS: Intrusion detection using process accounting records", *Journal of Computer Security*, Vol. 10, No. 2, pp. 159-176, 2002.
10. Spinellis D., Gritzalis S., Iliadis J., Gritzalis D., Katsikas S., "Trusted Third Party services for deploying secure telemedical applications over the WWW", *Computers & Security*, Vol. 18, No. 7, pp. 627-639, 1999.