WHEN TRUST MATTERS

Giới thiệu các quy định về an ninh mạng

Quản lý an ninh mạng trong ngành điện

DNV Singapore

07 August 2025



Chương trình

Thứ Năm- ngày 7/8/2025

SÁNG

- Giới thiệu các Quy định về An ninh mạng
  - Singapore
  - Chương trình Bảo vệ hạ tầng trọng yếu của Tập đoàn điện lực Bắc Mỹ (NERC CIP)
  - Liên minh châu Âu

CHIỀU

- Khía cạnh quy định về an ninh mạng
  - Cấu trúc quy định
  - Các yêu cầu quy định bắt buộc

Thứ Sáu- ngày 8/8/2025

SÁNG

- Yêu cầu quy định về an ninh mạng (1)
  - Quản trị (Kiểm toán)
  - Quản lý tài sản
  - Bảo vệ

CHIỀU

- Yêu cầu quy định về an ninh mạng (2)
  - Phát hiện
  - Ứng phó và Phục hồi
- Tóm tắt

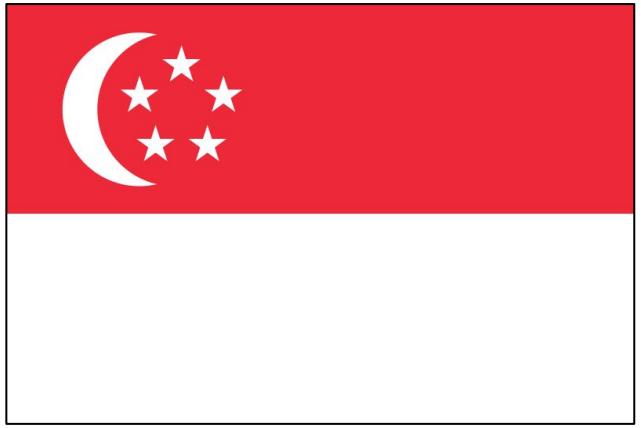
Luật an ninh mạng – Xu hướng thịnh hành

- Luật an ninh mạng hợp nhất là một xu hướng tương đối mới.
- Trước đây, các luật điều chỉnh vấn đề an ninh mạng còn rải rác và được quy định theo chủ đề:
  - Gian lận
  - Sử dụng máy tính sai mục đích
  - Bảo vệ dữ liệu cá nhân
- Hầu hết các luật này cho phép chính phủ điều tra và trừng phạt “tin tặc” và các hoạt động “hack”. Nhưng không áp đặt bất kỳ nghĩa vụ nào đối với đơn vị vận hành hệ thống khi bị “hack”.
- Theo khung pháp lý cũ, một người có thể bị kết tội vì đã có hành vi “hack” hệ thống, nhưng nạn nhân không thể bị kết tội “lơ là, thiếu sót”.

Luật an ninh mạng – Mục đích

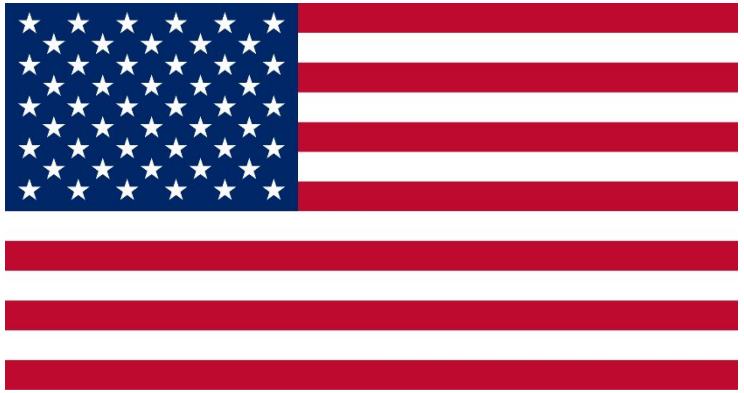
- Xem xét các mối đe dọa an ninh mạng ngày càng phổ biến và nổi bật, hầu hết các quốc gia hiện đang xây dựng hoặc thực hiện luật an ninh mạng hợp nhất.
- Trọng tâm của các luật an ninh mạng là đưa ra cách tiếp cận hợp nhất để quản lý rủi ro an ninh mạng ở cấp quốc gia.
- Đồng nghĩa với việc luật áp đặt nghĩa vụ bảo vệ hệ thống một cách phù hợp đối với các đơn vị vận hành hệ thống.
- Xác định chế tài đối với đơn vị vận hành hệ thống khi không tuân thủ chứ không chỉ trừng phạt “tin tặc”.
- Thành lập cơ quan quốc gia trung ương có trách nhiệm soạn thảo, triển khai và thực thi các chiến lược, tiêu chuẩn và hướng dẫn về an ninh mạng quốc gia.

Nghiên cứu điển hình về quy định



Singapore

- Bao gồm các quốc gia Khối thịnh vượng chung CA-TBD khác (Malaysia, Hồng Kông). Tuân thủ cùng khung pháp lý
- Đã hoàn thiện (thực thi từ năm 2018) và DNV Singapore có nhiều kinh nghiệm nhất



NERC-CIP

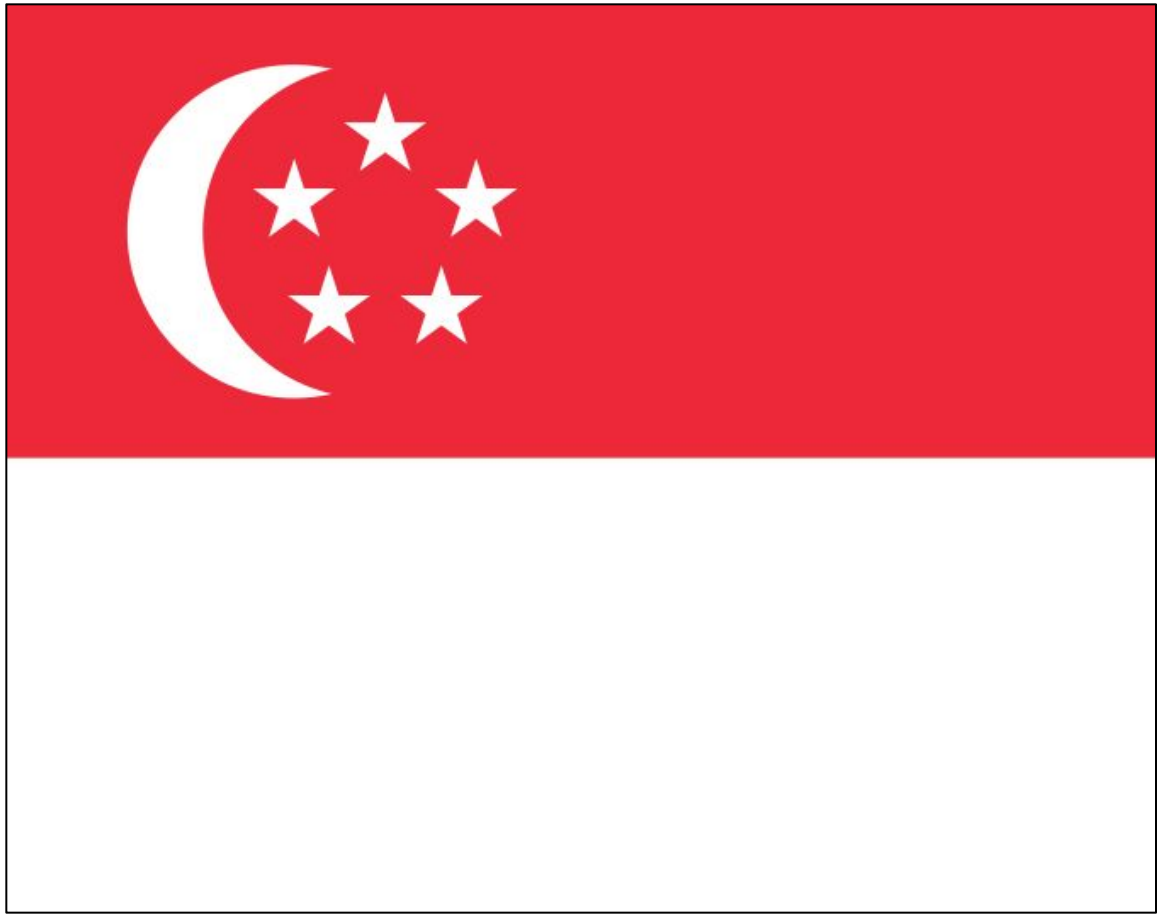
- Hoa Kỳ & Canada & Một số vùng thuộc Mexico
- Là một hợp tác xã được thành lập năm 1968 nhằm điều phối các công ty điện lực
- Đã hoàn thiện (dự thảo đầu tiên năm 2003)



Liên minh Châu Âu

- NIS2 - CHỈ THỊ (EU) 2022/2555 CỦA NGHỊ VIỆN VÀ HỘI ĐỒNG CHÂU ÂU
- CER - CHỈ THỊ (EU) 2022/2557 CỦA NGHỊ VIỆN VÀ HỘI ĐỒNG CHÂU ÂU

Khung pháp lý của Singapore

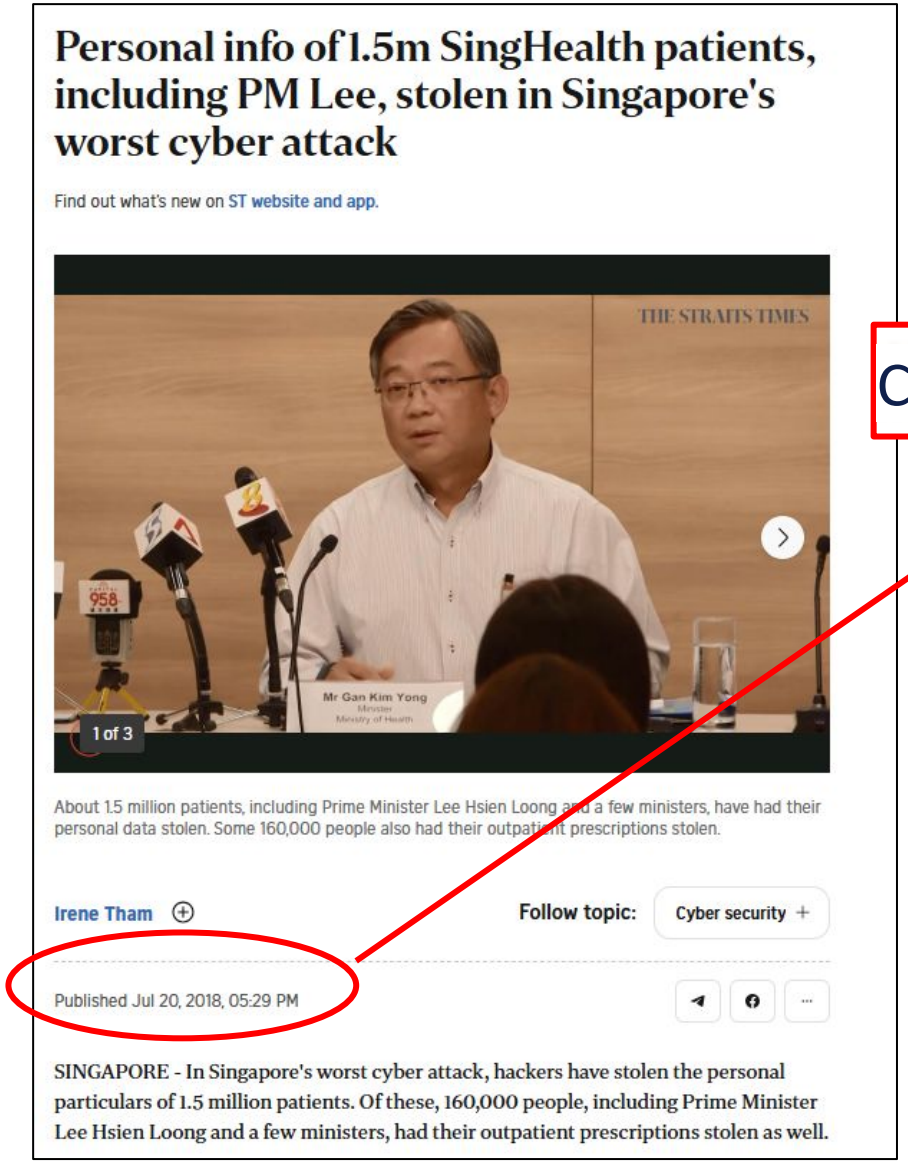


- Bao gồm các quốc gia Khối thịnh vượng chung CA-TBD khác (Malaysia, Hồng Kông). Tuân thủ cùng khung pháp lý
- Đã hoàn thiện (thực thi từ năm 2018) và DNV Singapore có nhiều kinh nghiệm nhất

Khung pháp lý của Singapore - Tổng quan

Quốc gia	Luật	Trạng thái luật	Lĩnh vực	Phạm vi	Cơ quan thực thi	Hướng dẫn
Singapore	Đạo luật An ninh mạng 2018	Đã thông qua. Đang có hiệu lực.	Hạ tầng thông tin trọng yếu (CII) đã chỉ định	• Biện pháp kiểm soát bắt buộc • Yêu cầu kiểm toán • Yêu cầu báo cáo	Cơ quan an ninh mạng Singapore (CSA)	Quy tắc hành vi an ninh mạng (CCoP)
Malaysia	Đạo luật An ninh mạng 2024	Đã thông qua. Đang có hiệu lực.	CII sẽ chỉ định sau		Cơ quan an ninh mạng quốc gia (NACSA)	Đang soạn thảo
Hồng Kông	Sắc lệnh Bảo vệ hạ tầng trọng yếu (Hệ thống máy tính) năm 2025	Đã thông qua; Có hiệu lực từ ngày 1/1/2026	Sẽ chỉ định sau - Có danh sách lĩnh vực cụ thể		Ủy viên Hạ tầng trọng yếu sẽ bổ nhiệm	Đang soạn thảo

Vì sao Singapore ban hành luật này sớm như vậy?



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

Find out what's new on ST website and app.

About 1.5 million patients, including Prime Minister Lee Hsien Loong and a few ministers, have had their personal data stolen. Some 160,000 people also had their outpatient prescriptions stolen.

Irene Tham

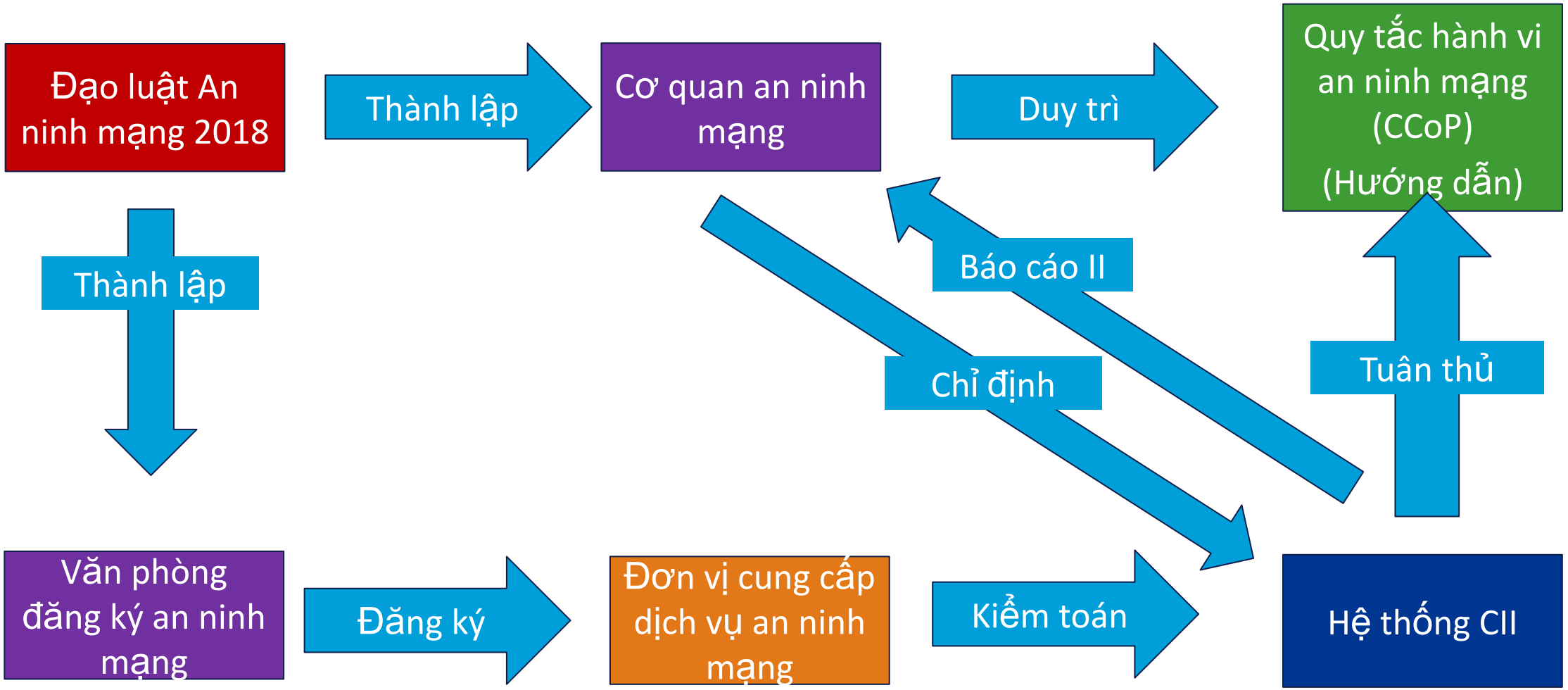
Follow topic: Cyber security +

Published Jul 20, 2018, 05:29 PM

SINGAPORE - In Singapore's worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.

Công bố ngày 20/7/2018, 17:29

Khung pháp lý của Singapore



Cơ quan An ninh mạng Singapore (CSA)

- https://www.csa.gov.sg/
- Cơ quan được thành lập theo Đạo luật An ninh mạng
- Vai trò của CSA bao gồm:
  - Soạn thảo và thực thi các hướng dẫn về an ninh mạng (CCoP)
  - Điều phối hoạt động ứng phó sự có an ninh mạng cùng doanh nghiệp
  - Theo dõi các sự cố an ninh mạng
  - Nâng cao nhận thức về an ninh mạng cấp quốc gia



Văn phòng Quản lý An ninh mạng (CSRO)

- https://www.csa.gov.sg/
- Cơ quan được thành lập theo Đạo luật An ninh mạng
- Đăng ký kiểm thử xâm nhập cho các công ty và cá nhân
- Đảm bảo tiêu chuẩn dịch vụ an ninh mạng tại Singapore
- (https://www.csro.gov.sg/how-to/apply-for-licence/)
- Cả DNV Singapore và tôi đều đã được cấp phép =)
  - list_of_licensed_business_entities_25jul.pdf
  - list_of_licensed_individuals_25jul.pdf



Các mục trong CCoP

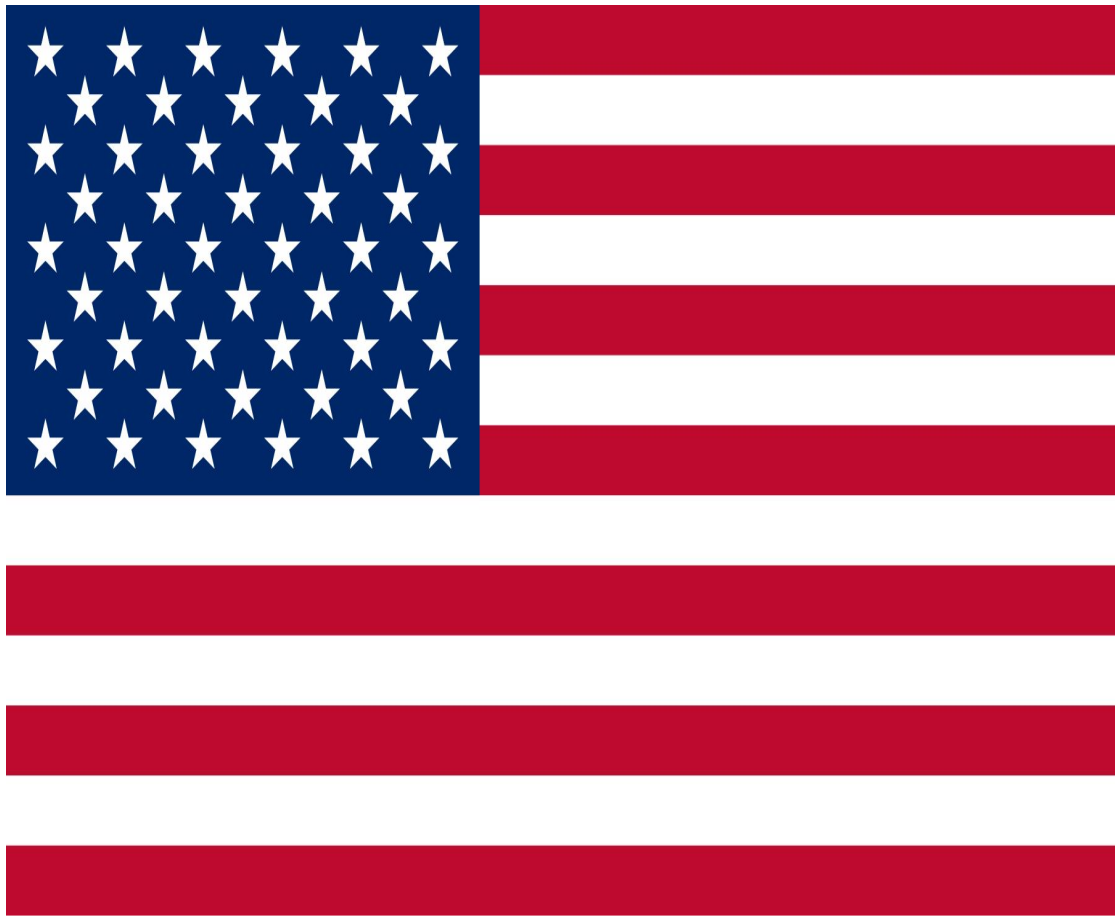
CCoP---Second-Edition_Revision-One.pdf

1. Thông tin sơ bộ
2. Yêu cầu về kiểm toán
3. Yêu cầu về quản trị
4. Yêu cầu về nhận dạng
5. Yêu cầu bảo vệ
6. Yêu cầu về phát hiện
7. Yêu cầu về ứng phó và phục hồi
8. Yêu cầu về khả năng phục hồi mạng
9. Đào tạo và nâng cao nhận thức về an ninh mạng
10. Yêu cầu về bảo mật công nghệ vận hành (OT)

Bộ quy tắc thực hành an ninh mạng (CCoP)

- CCoP---Second-Edition_Revision-One.pdf
- 10 mục nêu các yêu cầu
- Tập trung vào hệ thống, không phụ thuộc vào lĩnh vực, không phụ thuộc vào tiêu chuẩn ngành, được CSA chỉ định
- Rất cụ thể với các nhận định về loại thiết kế được chấp nhận.
  - “10.2.1 Đơn vị vận hành CII (CIIO) phải đảm bảo rằng hạ tầng thông tin trọng yếu (CII) của công nghệ vận hành (OT) không được kết nối với bất kỳ mạng doanh nghiệp nào, trừ khi cần thiết để vận hành hạ tầng thiết yếu và với điều kiện luồng dữ liệu chỉ giới hạn theo một chiều từ CII của OT đến mạng doanh nghiệp.”
  - Yêu cầu thực hiện phê duyệt thiết kế
  - ADMS không thể triển khai ở Singapore
- Trình độ của kiểm toán viên

Khung NERC-CIP

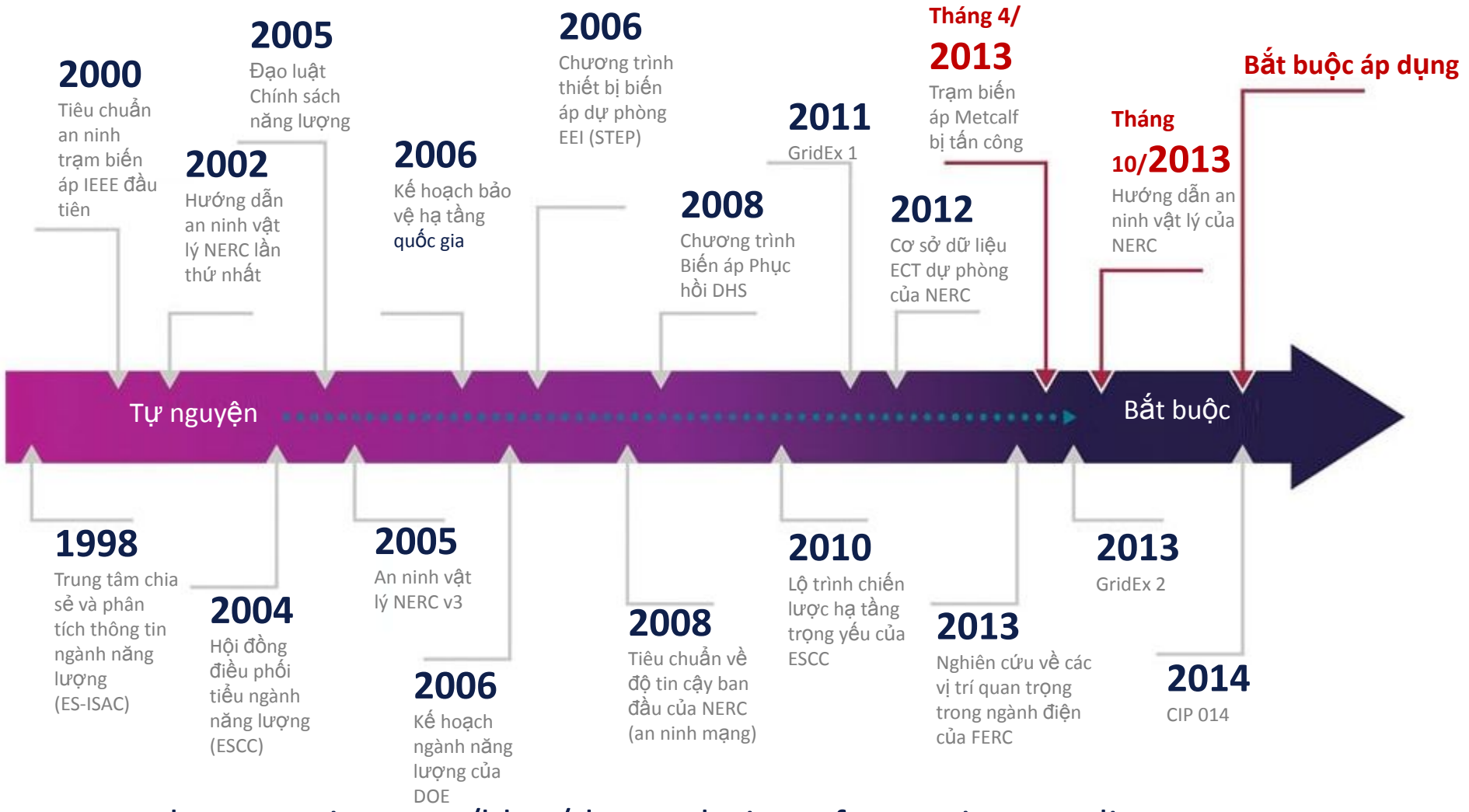


- Hoa Kỳ & Canada & Một số vùng thuộc Mexico
- Tập đoàn điện lực Bắc Mỹ (NERC) là một tổ chức hợp tác xã được thành lập năm 1968 nhằm điều phối các công ty điện lực
- Đã hoàn thiện (dự thảo đầu tiên năm 2003)

Tập đoàn Điện lực Bắc Mỹ (NERC)

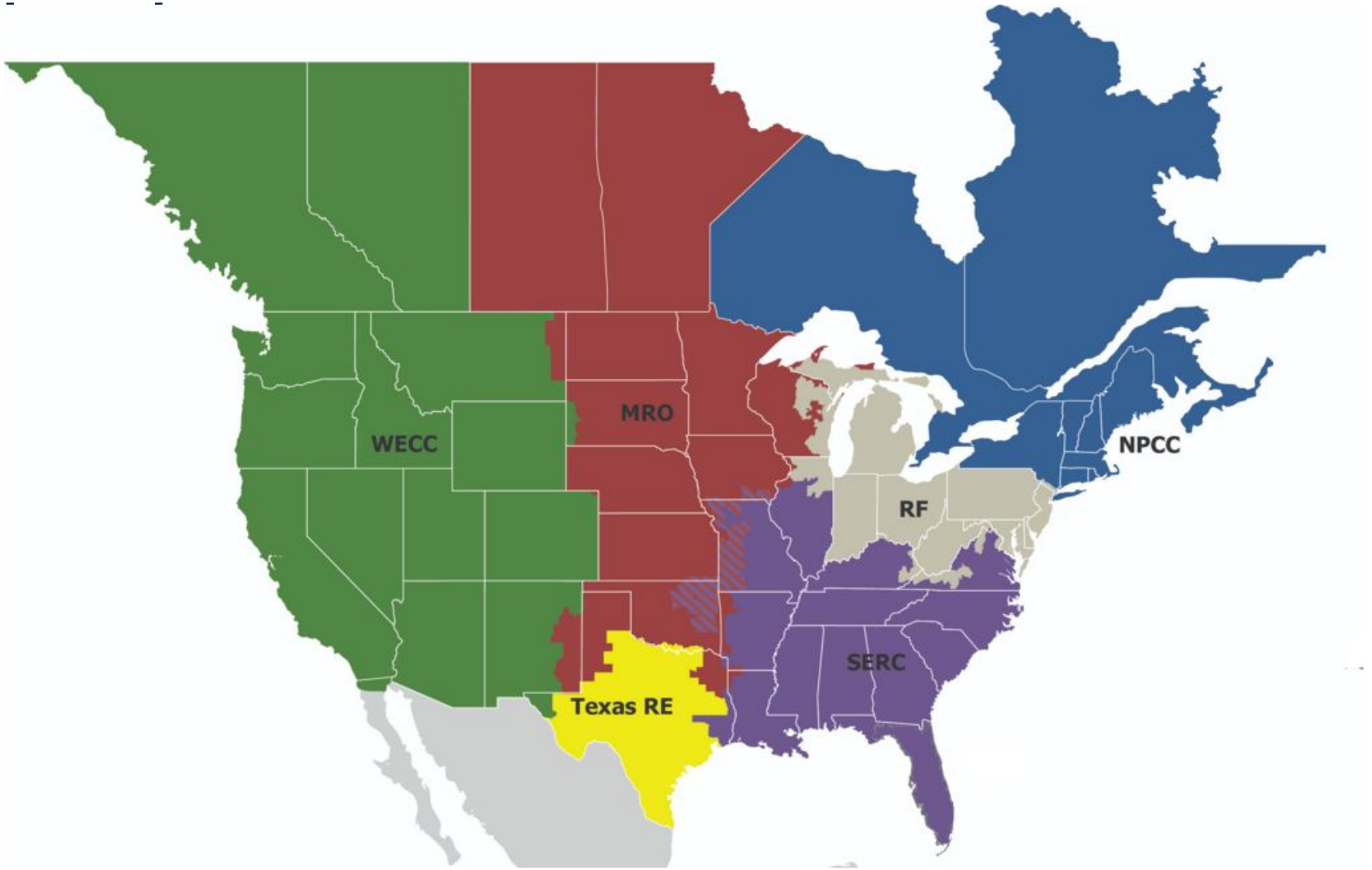
- NERC giám sát sáu đơn vị đảm bảo độ tin cậy của hệ thống điện khu vực, bao gồm tất cả các hệ thống điện kết nối của Canada và phần tiếp giáp Hoa Kỳ, cũng như một phần của tiểu bang Baja California của Mexico
- Đạo luật Chính sách năng lượng năm 2005 (Hoa Kỳ) kêu gọi thành lập **Tổ chức Độ tin cậy điện (ERO)** để xây dựng và thực thi các tiêu chuẩn bắt buộc về độ tin cậy tại Hoa Kỳ.
- Tháng 4/2006, NERC đã nộp đơn và được Ủy ban Điều tiết năng lượng liên bang (FERC) chỉ định giữ vai trò ERO vào tháng 7/2006
- Các tiêu chuẩn của NERC – CIP (Bảo vệ hạ tầng trọng yếu) là BẮT BUỘC theo luật, áp dụng với tất cả Hệ thống điện kết nối quy mô lớn (BES) ở Bắc Mỹ

Lịch sử phát triển NERC



- https://www.network-perception.com/blog/the-evolution-of-nerc-cip-compliance

6 đơn vị thuộc NERC



NERC-CIP

- https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
- Các tiêu chuẩn của NERC – CIP (Bảo vệ hạ tầng trọng yếu) là BẮT BUỘC theo luật, áp dụng với tất cả Hệ thống điện kết nối quy mô lớn (BES) ở Bắc Mỹ
- 14 tiêu chuẩn điều chỉnh các khía cạnh khác nhau trong an ninh mạng cho BES (Hệ thống điện kết nối quy mô lớn)
- Vai trò của NERC:
  - Phát triển chính sách (NERC-CIP)
  - Kiểm toán
  - Thực thi

Quốc gia	Luật	Trạng thái luật	Lĩnh vực	Phạm vi	Cơ quan thực thi	Chính sách
Hoa Kỳ và Canada	Đạo luật Chính sách năng lượng năm 2005	Đã thông qua. Đang có hiệu lực.	Hệ thống điện kết nối quy mô lớn	• Độ tin cậy năng lượng • An ninh mạng	NERC	NERC-CIP

NERC-CIP

- https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
- CIP-001 : Báo cáo vụ việc phá hoại
- CIP-002 : An ninh mạng – Phân loại hệ thống an ninh mạng của BES
- CIP-003 : An ninh mạng – Kiểm soát quản lý an ninh
- CIP-004 : An ninh mạng – Nhân sự & Đào tạo
- CIP-005 : An ninh mạng – Vành đai an ninh mạng điện tử
- CIP-006 : An ninh mạng – An ninh vật lý Hệ thống mạng của BES
- CIP-007 : An ninh mạng – Quản lý an ninh hệ thống
- CIP-008 : An ninh mạng – Báo cáo sự cố và lập kế hoạch ứng phó

BES: Hệ thống năng lượng kết nối quy mô lớn

NERC-CIP

- https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
- CIP-009 : Kế hoạch phục hồi cho Hệ thống mạng của BES
- CIP-010 : An ninh mạng – Quản lý thay đổi thành phần cấu hình và đánh giá lỗ hổng
- CIP-011 : An ninh mạng – Bảo vệ thông tin
- CIP-012 : An ninh mạng – Truyền thông giữa các trung tâm điều khiển
- CIP-013 : An ninh mạng – Quản lý rủi ro chuỗi cung ứng
- CIP-014 : An ninh mạng – An ninh vật lý
- CIP-015 : An ninh mạng – An ninh mạng – Giám sát an ninh mạng nội bộ (Chưa thực thi)

Khung pháp lý Liên minh Châu Âu



- NIS2 - CHỈ THỊ (EU) 2022/2555 CỦA NGHỊ VIỆN VÀ HỘI ĐỒNG CHÂU ÂU
- CER - CHỈ THỊ (EU) 2022/2557 CỦA NGHỊ VIỆN VÀ HỘI ĐỒNG CHÂU ÂU

Khung pháp lý Liên minh Châu Âu

NIS2

- Tập trung vào an ninh mạng
- Thiết lập các biện pháp an ninh mạng tiêu chuẩn



CER

- Tập trung nhiều hơn vào khả năng phục hồi của hệ thống. (Duy trì hoạt động và phục hồi sau thảm họa)
- Thiết lập các biện pháp phục hồi tiêu chuẩn

- Hai chỉ thị có điểm trùng nhau
- Cả hai đều xác định các lĩnh vực điều chỉnh
- Phần lớn trong chỉ thị đưa ra hướng dẫn để các quốc gia thành viên thông qua luật nhằm triển khai khả năng phục hồi của hệ thống đối với hạ tầng trọng yếu.
- Chỉ thị hướng dẫn các cơ sở tổ chức thực hiện và thực thi.
- Chi tiết sẽ được xác định ở cấp quốc gia sao cho phù hợp với các yêu cầu của EU.

NIS2 – Phạm vi

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
- Thành lập Đội ứng phó sự cố an ninh máy tính (CSIRT) quốc gia, bên cạnh các Cơ quan có thẩm quyền quốc gia (NCA) và các Đầu mối duy nhất (SPOC).
- Phạm vi giới hạn trong tổ chức
- Chỉ thị này chia các tổ chức thành hai loại:
  - **Các tổ chức thiết yếu** (VD: năng lượng, y tế, ngân hàng, giao thông vận tải) chịu sự giám sát và thực thi chặt chẽ hơn
  - **Các tổ chức quan trọng** (VD: dịch vụ CNTT, cơ sở hạ tầng kỹ thuật số, sản xuất) vẫn phải tuân thủ nhưng với mức độ giám sát theo quy định thấp hơn một chút
- Việc tổ chức thực hiện và chi tiết được xác định ở cấp quốc gia.
- Mức độ rất cao so với NERC-CIP hoặc Đạo luật an ninh mạng Singapore.

Yêu cầu của NIS2

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
- Chỉ thị bao gồm các điều khoản về:
  - Nghĩa vụ thông báo sự cố
  - Các biện pháp quản lý rủi ro an ninh mạng
  - Giám sát
  - Thực thi và chế tài
  - Trách nhiệm quản lý

NIS2 - Các biện pháp quản lý rủi ro an ninh mạng

1. Phân tích rủi ro và chính sách bảo mật thông tin
2. Xử lý sự cố
3. Duy trì hoạt động
4. Bảo mật chuỗi cung ứng
5. Xử lý và báo cáo về lỗ hổng
6. Các quy trình đánh giá hiệu quả quản lý rủi ro mạng
7. Thực hành vệ sinh máy tính và đào tạo an ninh mạng
8. Chính sách và quy trình về mật mã và mã hóa
9. An ninh liên quan đến nhân sự, chính sách kiểm soát truy cập và quản lý tài sản
10. Sử dụng xác thực đa yếu tố và hệ thống truyền thông an toàn

Khả năng phục hồi của các tổ chức trọng yếu (CER)

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
- Phần lớn trong chỉ thị đưa ra hướng dẫn để các quốc gia thành viên thông qua luật nhằm triển khai khả năng phục hồi của hệ thống đối với hạ tầng trọng yếu.
- Tập trung nhiều hơn vào khả năng phục hồi của hệ thống. (Duy trì hoạt động và phục hồi sau thảm họa)
- Các quốc gia thành viên vẫn phải thông qua luật để chỉ thị này có hiệu lực tại các quốc gia thành viên.

Khả năng phục hồi của các tổ chức trọng yếu (CER)

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
- 29 điều trong 8 chương
- Liệt kê 11 lĩnh vực
  - Lĩnh vực năng lượng
  - Lĩnh vực vận tải
  - Lĩnh vực ngân hàng
  - Lĩnh vực hạ tầng thị trường tài chính
  - Lĩnh vực y tế
  - Lĩnh vực nước uống
  - Lĩnh vực nước thải
  - Lĩnh vực hạ tầng số
  - Lĩnh vực dịch vụ hành chính công
  - Lĩnh vực vũ trụ
  - Lĩnh vực sản xuất, chế biến và phân phối thực phẩm

Khả năng phục hồi của các tổ chức trọng yếu (CER) – Các điều khoản chính (1)

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

- Các chương chính:
  - CHƯƠNG II, KHUNG QUỐC GIA VỀ KHẢ NĂNG PHỤC HỒI CỦA CÁC TỔ CHỨC TRỌNG YẾU
    - Điều 4, Chiến lược về khả năng phục hồi của các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 5, Đánh giá rủi ro của các quốc gia thành viên, Chỉ thị CER.
    - Điều 6, Xác định các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 7, Tác động mang tính gián đoạn lớn, Chỉ thị CER.
    - Điều 8, Các tổ chức trọng yếu trong lĩnh vực ngân hàng, hạ tầng thị trường tài chính và hạ tầng số, Chỉ thị CER.
    - Điều 9, Cơ quan có thẩm quyền và đầu mối duy nhất, Chỉ thị CER.
    - Điều 10, Hỗ trợ của các quốc gia thành viên cho các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 11, Hợp tác giữa các quốc gia thành viên, Chỉ thị CER.

Khả năng phục hồi của các tổ chức trọng yếu (CER) – Các điều khoản chính (2)

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
- Các chương chính:
  - CHƯƠNG III, BIỆN PHÁP PHỤC HỒI CỦA CÁC TỔ CHỨC TRỌNG YẾU
    - Điều 12, Đánh giá rủi ro của các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 13, Biện pháp phục hồi của các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 14, Kiểm tra thông tin cơ bản, Chỉ thị CER.
    - Điều 15, Thông báo sự cố, Chỉ thị CER.
    - Điều 16, Tiêu chuẩn, Chỉ thị CER.
  - CHƯƠNG IV, CÁC TỔ CHỨC TRỌNG YẾU CÓ Ý NGHĨA ĐẶC BIỆT ĐỐI VỚI CHÂU ÂU
    - Điều 17, Xác định các tổ chức trọng yếu có ý nghĩa đặc biệt đối với châu Âu, Chỉ thị CER.
    - Điều 18, Nhiệm vụ cố vấn, Chỉ thị CER.

Khả năng phục hồi của các tổ chức trọng yếu (CER) – Các điều khoản chính (3)

- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
- Các chương chính:
  - CHƯƠNG V, HỢP TÁC VÀ BÁO CÁO
    - Điều 19, Nhóm phục hồi các tổ chức trọng yếu, Chỉ thị CER.
    - Điều 20, Hỗ trợ của Ủy ban Châu Âu cho các cơ quan có thẩm quyền và các tổ chức trọng yếu, Chỉ thị CER.
  - CHƯƠNG VI, GIÁM SÁT VÀ THỰC THI
    - Điều 21, Giám sát và thực thi, Chỉ thị CER.
    - Điều 22, Chế tài, Chỉ thị CER.

Trên tin tức…..

https://plesner.com/en/news/denmark-introduces-cer-act-strengthen-resilience-critical-entities

Denmark introduces CER Act to strengthen resilience of critical entities

Legal News 20.06.2025



Niklas Korsgaard Christensen
Attorney-at-Law (H), Managing Partner, MBA



Jacob Ørskov Rasmussen
Attorney-at-Law, Partner





On 1 July 2025, Denmark's Act on the Resilience of Critical Entities (the "CER Act") enters into force. The Act transposes the CER Directive (Directive (EU) 2022/2557) and introduces binding resilience requirements for critical entities essential to societal functions, including utility providers and infrastructure operators.

Key implications

The CER Act transposes the Critical Entities Resilience Directive (Directive (EU) 2022/2557) and introduces binding resilience

Tài liệu tham khảo

- NIS2
  - Văn bản luật: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
  - Tóm tắt:
    - https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/10/kpmg-network-and-information-security-directive-nis2.pdf
    - https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
    - https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
- CER
  - Văn bản luật: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
  - Tóm tắt:
    - https://ec.europa.eu/newsroom/cipr/items/764849/en
    - https://www.critical-entities-resilience-directive.com/
    - https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

Giới thiệu các Quy định về An ninh mạng

Quản lý an ninh mạng trong ngành điện

Wei.Ming.Quek@dnv.com
+65 9827 8699

www.dnv.com