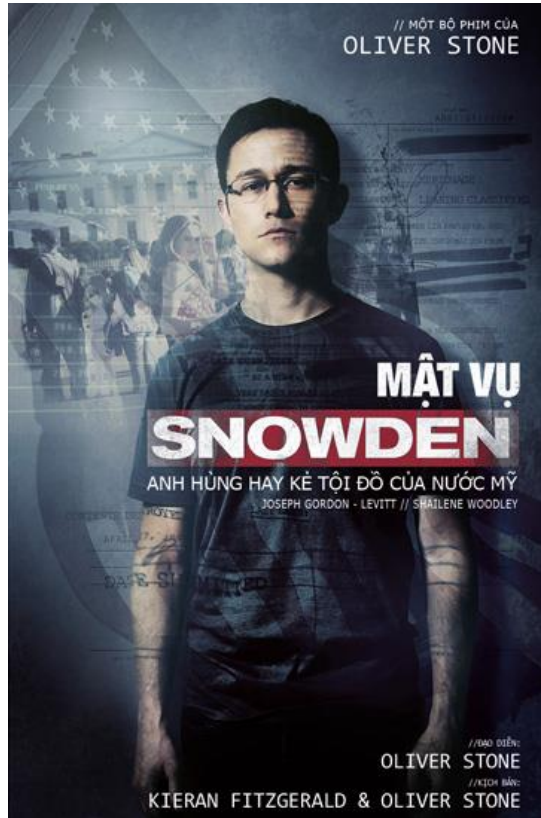




QUẢN LÝ AN TOÀN THÔNG TIN

NHÂN SỰ VÀ AN TOÀN




Edward Joseph Snowden

Ted talk



GIỚI THIỆU CHUNG

- 
- Duy trì một môi trường an toàn đòi hỏi bộ phận bảo mật thông tin phải được cấu trúc cẩn thận và có nhân viên có chứng chỉ phù hợp

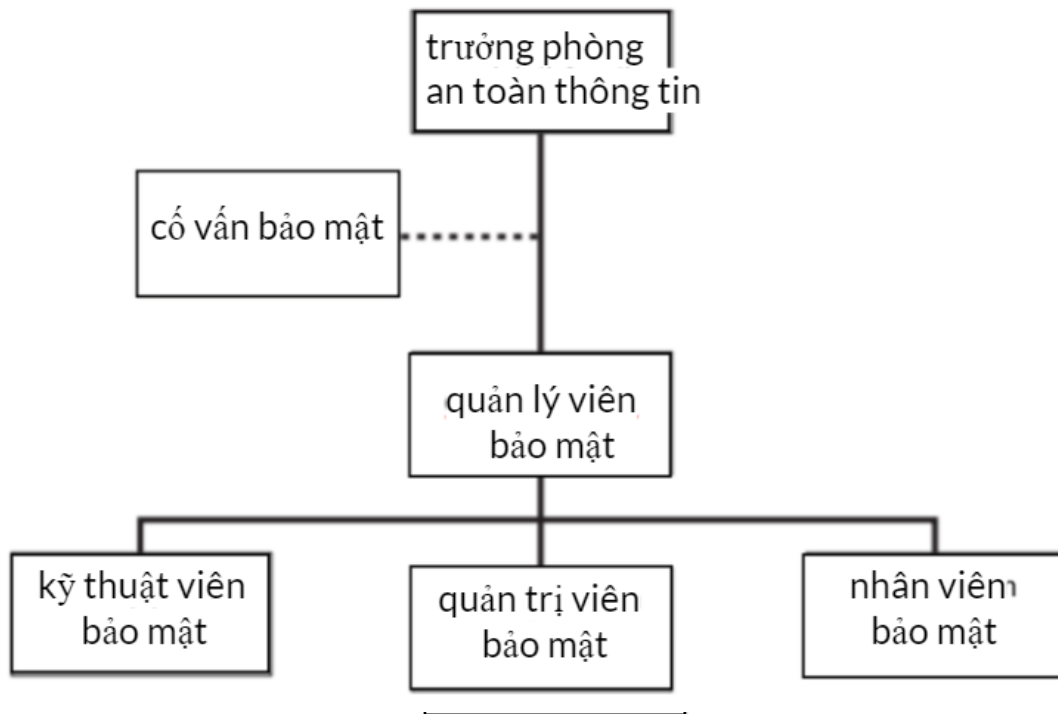
CÁC VỊ TRÍ- CHỨC VỤ TRONG ATTT

- Các loại chức vụ trong bảo mật thông tin

- Đánh giá
- Xây dựng
- Quản trị

- Chức vụ phổ biến

- CISO
- Quản lý bảo mật
- Kỹ thuật viên bảo mật



- Đứng đầu về ATTT

- Hiểu rõ về chính sách, chiến lược, thông thạo mọi lĩnh vực

- Trao đổi trực tiếp với CIO Giám đốc thông tin

- Chịu trách nhiệm về phát ngôn hay chương trình chung của ATTT

Các yêu cầu về trình độ và vị trí

Các bằng cấp phổ biến nhất cho CISO bao gồm:

- (CISSP - the Certified Information Systems Security Professional) *Chuyên gia Bảo mật Hệ thống Thông tin*

- (CISM - the Certified Information Security Manager) *Người Quản lý Bảo mật Thông tin*

- Bằng kinh doanh, công nghệ
- Quản lý bảo mật
- Lập kế hoạch, chính sách và ngân sách.
- Kinh nghiệm thực thi pháp luật

Bộ phận an toàn thông tin

- Trách nhiệm và nhiệm vụ: bảo đảm ATTT các thông tin về công ty (chính sách, phần cứng, phần mềm, tài liệu, ...)
- Vấn đề liên quan tới ATTT: lỗ hổng bảo mật, biện pháp kiểm soát, công nghệ, vấn đề về con người và quản lý
- Phòng làm việc với các bộ phận khác liên quan tới vấn đề ATTT

Quản lý viên an ninh

- Chịu trách nhiệm hoạt động thường ngày của ATTT
- Nhận nhiệm vụ từ CISO và hoàn thành (ví dụ như lớp trưởng trong lớp học, thầy là CISO)
- Xử lý các công việc được phản ánh từ nhân viên kỹ thuật
- Am hiểu về công nghệ, kỹ thuật (không cần quá sâu, chi tiết)
- Duy trì, phát triển kiến thức → quản lý, sáng kiến

Quản lý viên an ninh

Nhiệm vụ với tổ chức:

- Làm việc với các phòng ban, cơ quan khác
- Giám sát, lập kế hoạch
- Giải quyết vấn đề phát sinh
- Sàng lọc, tuyển dụng
- Phân công vị trí, công việc

Yêu cầu trình độ, chứng chỉ:

- CISSP, CISM
- Chuyên môn hóa hơn so với CISO (vai trò khác nhau thì có sự chuyên môn khác nhau)
- Quản lý nhân sự, tuyển dụng, lập kế hoạch,...

Kỹ thuật viên an ninh

- Trình độ kỹ thuật chuyên sâu: cấu hình tường lửa, triển khai phần mềm bảo mật, chuẩn đoán và khắc phục sự cố
- Kinh nghiệm với công nghệ đó
- Thành thạo về công nghệ, công cụ cụ thể

THÔNG TIN VỀ CHỨNG CHỈ CHUYÊN NGHIỆP

- Nhiều tổ chức dựa vào chứng chỉ chuyên môn để xác định mức độ thành thạo của ứng viên.
- Các chứng chỉ không phản ánh chính xác hoàn toàn năng lực của ứng viên.
- Nhân viên ATTT sẽ xác định chứng chỉ nào sẽ phù hợp với họ trong thị trường việc làm.

CÁC LOẠI CHỨNG CHỈ PHỔ BIẾN

- Chứng chỉ CISSP
- Chứng chỉ SSCP
- Chứng chỉ CSSLP
- Chứng chỉ ISACA
- Chứng chỉ CISA
- Chứng chỉ CGEIT
- Chứng chỉ CompTIA
- Chứng chỉ GIAC

(ISC)2 là gì?

(ISC)²

Tổ chức phi lợi nhuận



(ISC)²®

(ISC)2: International Information System Security Certification Consortium

Là tổ chức chứng nhận bảo mật hệ thống thông tin quốc tế.

Là một tổ chức phi lợi nhuận chuyên đào tạo và chứng nhận cho các chuyên gia an ninh mạng quốc tế

Chứng chỉ CISSP (*Certified Information Systems Security Professional*): Chuyên gia Bảo mật Hệ thống Thông tin.

- Đây là chứng chỉ cao cấp dành cho các chuyên gia về bảo mật muốn chứng minh rằng họ có thể thiết kế, triển khai và quản lý một chương trình an ninh mạng ở cấp doanh nghiệp.
- Chứng chỉ này được cung cấp bởi (ISC)2.

8 lĩnh vực kiến thức cần có cho CISSP

- Quản lý bảo mật và quản lý rủi ro
- Bảo mật tài sản
- Kỹ thuật và kiến trúc bảo mật
- Truyền thông và an ninh mạng
- Quản lý định danh và truy cập (IAM)
- Đánh giá bảo mật và kiểm thử
- Bảo mật trong vận hành
- Bảo mật trong phát triển phần mềm

Các yêu cầu để nhận chứng chỉ CISSP

Có 2 yêu cầu chính: ***Làm bài kiểm tra*** và ***Kinh nghiệm***

Kỳ thi CISSP gồm:

- 250 câu hỏi trắc nghiệm trong vòng sáu giờ.
- Bao gồm 10 lĩnh vực kiến thức InfoSec (An toàn thông tin).

Kinh nghiệm: Bạn cần có 5 năm kinh nghiệm làm việc toàn thời gian với ít nhất 2 trong 8 lĩnh vực CISSP.

<https://www.isc2.org/Certifications/CISSP/experience-requirements>

Các chi phí của chứng chỉ CISSP

- Tiền tham gia các khóa học.
- 599-699 đô la để tham dự kỳ thi.
- Để duy trì chứng chỉ CISSP của bạn, bạn cần phải trả một khoản phí duy trì hàng năm là 125 đô la.

Các chứng chỉ chuyên môn của CISSP

- **ISSAP®**: Kiến trúc bảo mật hệ thống thông tin chuyên nghiệp
 - Hệ thống kiểm soát truy cập và phương pháp luận
 - Viễn thông và an ninh mạng
 - Mật mã học
 - Phân tích kiến trúc bảo mật
 - Lập kế hoạch kinh doanh liên tục liên quan đến công nghệ và lập kế hoạch khắc phục thảm họa
 - Tích hợp bảo mật vật lý

Các chứng chỉ chuyên môn của CISSP

- **ISSEP®**: Chuyên gia kỹ thuật bảo mật hệ thống thông tin
 - Kỹ thuật bảo mật hệ thống
 - Khung chứng nhận và công nhận/quản lý rủi ro
 - Quản lý kỹ thuật
 - Các chính sách và phát hành liên quan đến đảm bảo thông tin của chính phủ Hoa Kỳ

Các chứng chỉ chuyên môn của CISSP

ISSMP®: Hệ thống thông tin Quản lý bảo mật doanh nghiệp chuyên nghiệp Thực hành quản lý bảo mật

- Lập kế hoạch kinh doanh liên tục và lập kế hoạch khắc phục thảm họa
- Thực hành quản lý bảo mật
- Bảo mật phát triển hệ thống
- Luật pháp, điều tra, pháp y và đạo đức
- Quản lý tuân thủ bảo mật

Các chứng chỉ chuyên môn của CISSP

- **SSCP**(*Systems Security Certified Practitioner*): Chứng chỉ về bảo mật hệ thống.
 - Điều khiển truy nhập
 - Mật mã học
 - Mã độc và hoạt động
 - Giám sát và phân tích
 - Mạng và viễn thông
 - Rủi ro, phản ứng và phục hồi
 - Hoạt động và quản trị an ninh
- **CSSLP**(*Certified Secure Software Lifecycle Professional*): Chứng chỉ an toàn phần mềm vòng đời.

CHỨNG CHỈ BẢO MẬT THÔNG TIN TOÀN CẦU

GIAC(*Global Information Assurance Certification*) bao gồm:

- Chuyên gia bảo mật thông tin GIAC (GISP)
- Chứng nhận Lãnh đạo Bảo mật GIAC (GSLC)
- Chứng nhận Chuyên gia ISO-27000 GIAC (G2700)
- Chứng nhận Quản lý Dự án GIAC (GCPM)

Yêu cầu của chứng chỉ GIAC

Để nhận được chứng chỉ **GIAC** cần:

Hoàn thành 1 bài tập thực tế → Bài kiểm tra trực tuyến

3 loại chứng nhận:

- Bạc
- Vàng
- Bạch Kim

Chứng chỉ C|CISO

C|CISO được cung cấp bởi hệ thống chứng chỉ ***EC-Council***

C|CISO kiểm tra không chỉ kiến thức về lĩnh vực bảo mật mà còn cả kiến thức quản lý kinh doanh điều hành.

- Các lĩnh vực:
- Quản trị (Chính sách, Pháp lý và Tuân thủ)
 - Kiểm soát quản lý IS và Quản lý kiểm toán
 - Quản lý (Dự án và Vận hành)
 - Năng lực cốt lõi về bảo mật thông tin
 - Lập kế hoạch chiến lược và tài chính

Chứng chỉ CompTIA

CompTIA (*Computing Technology Industry Association*): được cấp từ Hiệp hội Công nghiệp Công nghệ Máy tính (CompTIA).

- Kỳ thi bao gồm:
- Chủ đề toàn ngành
 - Bảo mật truyền thông
 - Bảo mật cơ sở hạ tầng
 - Mật mã, kiểm soát truy cập, xác thực
 - Tấn công bên ngoài và bảo mật hoạt động và tổ chức

Chứng chỉ CompTIA

Bài kiểm tra gồm 6 lĩnh vực dưới đây:

Lĩnh vực	Tỷ lệ phần trăm kiểm tra
1.0 Bảo mật mạng	21%
2.0 Tuân thủ và bảo mật hoạt động	18%
3.0 Các mối đe dọa và lỗ hổng	21%
4.0 Ứng dụng, dữ liệu và bảo mật máy chủ	16%
5.0 Kiểm soát truy cập và Quản lý danh tính	13%
6.0 Mật mã	11%

Chứng chỉ CCE

CCE ®(*Certified Computer Examiner*): Là chứng nhận pháp y máy tính được cung cấp bởi **ISFCE**(*International Society of Forensic Computer Examiners*)

Điều kiện để cấp chứng chỉ **CCE**:

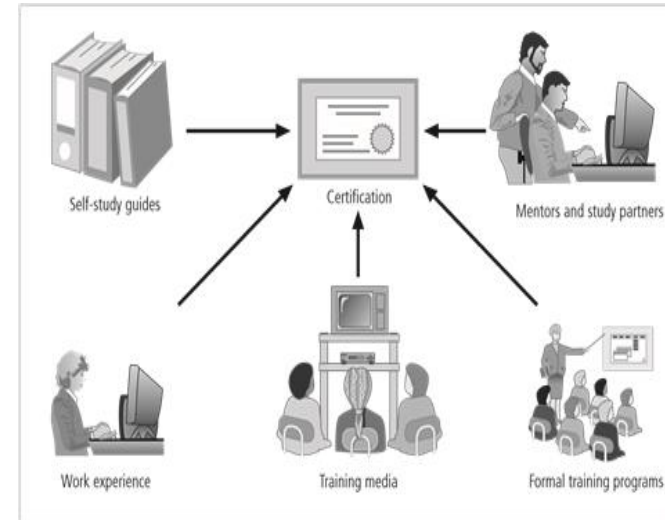
- Chưa có tiền án tiền sự
- Đáp ứng các yêu cầu kinh nghiệm, đào tạo hoặc tự đào tạo tối thiểu
- Tuân thủ quy tắc chứng nhận của các tiêu chuẩn đạo đức
- Vượt qua kỳ thi trực tuyến
- Thực hiện thành công giám định pháp y thực tế trên ba phương tiện xét nghiệm

Các lĩnh vực của chứng chỉ CCE

- Đạo đức trong thực tiễn
- Luật pháp và tác động của nó đối với pháp y kỹ thuật số
- Cấp phép và xác thực phần mềm
- Phần cứng máy tính nói chung được sử dụng trong thu thập dữ liệu
- Mạng và sự tham gia của nó trong pháp y và thu thập dữ liệu
- Hoạt động máy tính phổ biến và tổ chức hệ thống tệp và kiến trúc
- Thủ tục thu giữ dữ liệu pháp y
- Casework và các thủ tục giám định pháp y khác
- Phương tiện truyền thông máy tính phổ biến được sử dụng làm bằng chứng, hoạt động phương tiện lưu trữ vật lý và logic và quy trình khử trùng và sử dụng
- Sử dụng đĩa khởi động pháp y
- Kỹ năng và thủ tục giám định pháp y

TỔNG QUAN VỀ CHI PHÍ CHỨNG CHỈ

- Chứng chỉ tốt thì sẽ hơi tốn kém
- Chứng chỉ được các chuyên gia công nhận trong lĩnh vực của họ
- Chi phí cao làm cản trở những người có mong muốn kiểm tra đánh giá năng lực của bản thân
- Yêu cầu từ hai đến ba năm kinh nghiệm
- Cấu trúc các bài kiểm tra gồm nhiều lĩnh vực
- Quá trình cung cấp chứng chỉ phức tạp



CHÍNH SÁCH VÀ THỰC TRẠNG VIỆC LÀM

- Quản lý nhân sự nên tích hợp các khái niệm bảo mật thông tin an toàn trên tất cả các chính sách, điều khoản về việc làm của tổ chức bao gồm:
 - + Trách nhiệm bảo mật thông tin được đưa vào mô tả công việc của mọi nhân viên
 - + Đánh giá hiệu suất làm việc theo mỗi đợt

BẢO MẬT LÀ MỘT PHẦN CỦA ĐÁNH GIÁ HIỆU SUẤT

- Các tổ chức nên kết hợp các thành phần bảo mật thông tin vào đánh giá hiệu suất của nhân viên để nhân viên của mình làm việc tốt mà vẫn đảm bảo được về an toàn thông tin của công việc.

VẤN ĐỀ CHẤM DỨT

- Khi một nhân viên rời khỏi một tổ chức, các nhiệm vụ sau đây phải được thực hiện:

VẤN ĐỀ CHẤM DỨT - TRƯỜNG HỢP KHÔNG TỰ NGUYỆN

- Bảo mật cắt đứt tất cả quyền truy cập hệ thống và khóa thẻ trước khi nhân viên bị chấm dứt
- Nhân viên được báo cáo chấm dứt công việc và được hộ tống vào văn phòng an ninh để nhận tin chấm dứt việc làm
- Cá nhân sau đó được hộ tống khỏi nơi làm việc và được thông báo rằng tài sản cá nhân của họ sẽ được di chuyển hoặc được mang đến văn phòng, tủ hoặc khu vực cá nhân của cá nhân đó để có thể sắp xếp mang đi dưới sự giám sát của cơ quan, tổ chức.

VẤN ĐỀ CHẤM DỨT- TRƯỜNG HỢP TỰ NGUYỆN

- Hệ thống an ninh sẽ tước bỏ hết quyền truy cập và thẻ trước khi nhân viên bị sa thải
- Nhân viên có thể đã được thông báo trước ngày sa thải thực tế

Tài khoản nhân viên thường được phép tiếp tục, với ngày hết hạn mới

Nhân viên có thể đến và đi theo ý muốn

-Thường gói ghém hết tất cả đồ đạc và rời đi mà không phải họp tổng, nhưng phải để lại tất cả các tài sản tổ chức trước khi đi

VẤN ĐỀ CHẤM DỨT

- Trong cả hai trường hợp:
 - Văn phòng và thông tin được sử dụng bởi nhân viên rời đi phải được kiểm kê, các tập tin của họ được lưu trữ hoặc phá hủy và tất cả tài sản được trả lại cho các cơ quan, tổ chức họ từng làm việc
 - Nhân viên rời đi có thể sẽ đem về nhà thông tin hoặc tài sản có thể có giá trị trong công việc tương lai của họ
 - Xem xét kỹ lưỡng nhật ký hệ thống, có thể cho phép một tổ chức xác định xem vi phạm chính sách hoặc mất thông tin đã xảy ra

VẤN ĐỀ BẢO MẬT NHÂN SỰ

- Phương pháp giám sát và kiểm soát nhân viên
 - Tách biệt nhiệm vụ
 - Kiểm soát hai người
 - Luân chuyển công việc
 - Xoay nhiệm vụ

BẢO MẬT NHÂN SỰ & DỮ LIỆU CÁ NHÂN

- Các tổ chức được pháp luật yêu cầu bảo vệ thông tin nhạy cảm hoặc cá nhân của nhân viên
 - Trách nhiệm bảo mật mở rộng cho khách hàng và bất cứ ai mà tổ chức có mối quan hệ kinh doanh
- . * Dữ liệu nhân sự không khác gì các dữ liệu khác mà bảo mật thông tin có trách nhiệm cần phải bảo vệ

CÂN NHẮC BẢO MẬT NHÂN VIÊN KHÔNG CHÍNH THỨC

- Nhiều cá nhân không phải là nhân viên thường có quyền truy cập vào thông tin tổ chức nhạy cảm

CÂN NHẮC BẢO MẬT NHÂN VIÊN KHÔNG CHÍNH THỨC

- **Nhân viên tạm thời:**

- Không được tuyển dụng bởi tổ chức mà họ đang làm việc
- Có thể không phải tuân theo các nghĩa vụ hoặc chính sách hợp đồng chi phối nhân viên
- Trừ khi được quy định trong hợp đồng với tổ chức, cơ quan tạm thời có thể không chịu trách nhiệm về những tổn thất do người lao động gây ra.
- Việc tiếp cận thông tin nên được giới hạn ở những gì cần thiết để thực hiện nhiệm vụ của họ

CÂN NHẮC BẢO MẬT NHÂN VIÊN CHÍNH THỨC

- **Nhân viên theo hợp đồng**

- Biết những gì họ cần truy cập vào

Quy định về hợp đồng dịch vụ hoặc hợp đồng:

- Yêu cầu thông báo từ 24 đến 48 giờ
- Yêu cầu tất cả nhân viên tại chỗ phải trải qua kiểm tra lý lịch
- Yêu cầu thông báo trước để hủy bỏ hoặc lên lịch lại việc kiểm tra lý lịch

CÂN NHẮC BẢO MẬT NHÂN VIÊN KHÔNG CHÍNH THỨC

- **Tư vấn viên:**

- Có các nghĩa vụ bảo mật theo hợp đồng riêng
- Bảo vệ thông tin của bạn có thể không phải là ưu tiên số một của họ
- Áp dụng các nguyên tắc ít đặc quyền nhất