

QUẢN LÝ AN TOÀN THÔNG TIN

Giảng viên: Nguyễn Ngọc Diệp

LUẬT VÀ ĐẠO ĐỨC

Law & Ethics


Nội dung chính:

I. Giới thiệu về pháp luật và đạo đức ATTT

II. Luật quốc tế về ATTT

III. Vấn đề đạo đức ATTT

IV. Quản lý các cuộc điều tra trong một tổ chức



I: Giới thiệu về pháp luật và đạo đức ATTT

Giới thiệu

- Các chính sách, pháp luật và đạo đức con người đóng vai trò rất quan trọng trong việc đảm bảo an toàn cho thông tin, hệ thống và mạng.
- Các nhân viên đảm bảo an toàn cho thông tin cần hiểu rõ phạm vi, những khía cạnh pháp lý và đạo đức ATTT.
 - Nắm vững hệ thống, môi trường pháp lý hiện tại, các luật và quy định luật pháp.
 - Thực hiện công việc nằm trong khuôn khổ pháp luật.

Giới thiệu

- Cần thực hiện giáo dục ý thức về pháp luật và đạo đức ATTT cho cán bộ quản lý và nhân viên trong tổ chức, đảm bảo sử dụng đúng mục đích các công nghệ đảm bảo ATTT.

Luật (Law)

Luật: Gồm những điều khoản bắt buộc hoặc cấm những hành vi cụ thể.

- Thường được xây dựng từ các vấn đề đạo đức.
- Các kiểu luật:
 - Luật dân sự (Civil law)
 - Luật hình sự (Criminal law)

PHÂN LOẠI LUẬT

1.

Luật dân sự

Bao gồm nhiều loại luật liên quan đến các mối quan hệ giữa các cá nhân và tổ chức

2.

Luật hình sự

Những hành vi có hại cho xã hội được nhà nước truy tố

3.

Luật tra tấn

Cho phép các cá nhân yêu cầu giải quyết về bị thương về cá nhân, thể chất hoặc tài chính. Được thực thi tại tòa án dân sự và không bị truy tố

4.

Luật riêng tư

Điều chỉnh các mối quan hệ giữa các cá nhân và các tổ chức. Bao gồm luật gia đình, luật thương mại và luật lao động

5.

Luật công

Quy định cấu trúc và quản lý các cơ quan chính phủ và các mối quan hệ của họ với công dân, nhân viên và các chính phủ khác. Luật công bao gồm: luật hình sự, luật hành chính và luật hiến pháp

Luật (Law) tiếp

- So sánh giữa luật dân sự và hình sự

Cơ sở để so sánh	Luật dân sự	Pháp luật hình sự
Ý nghĩa	Luật dân sự đề cập đến một luật chung, liên quan đến tranh chấp giữa các cá nhân, tổ chức hoặc cả hai trong đó người phạm tội bồi thường cho người bị ảnh hưởng.	Luật hình sự bao hàm luật pháp liên quan đến các hành vi phạm tội hoặc tội ác đối với toàn xã hội.
Nội dung	Nguyên đơn	Chính quyền
Mục đích	Để duy trì quyền của một người và bồi thường cho anh ta.	Để duy trì luật pháp và trật tự, bảo vệ xã hội và đưa ra hình phạt cho những kẻ phạm tội.
Bắt đầu với	Nội đơn khởi kiện lên tòa án hoặc tòa án tương ứng, bởi bên bị kích động.	Đầu tiên, một khiếu nại được gửi đến cảnh sát điều tra tội phạm, sau đó, một vụ án được đệ trình lên tòa án.
Giao dịch với	Nó liên quan đến bất kỳ tác hại hoặc vi phạm quyền cá nhân.	Nó liên quan đến các hành vi mà pháp luật định nghĩa là hành vi phạm tội.
Hoạt động	Kiểm	Khởi tố
Kết quả	Biện pháp khắc phục	Trừng phạt

Chính sách (Policies) và Luật

- Chính sách (quy định, nội quy) là những mục tiêu mà một tổ chức hoặc chính phủ đặt ra cho mình để đạt được trong một khoảng thời gian nhất định
- Chính sách là các “luật” của tổ chức có giá trị thực thi trong nội bộ, gồm một tập các quy định và các chế tài xử phạt bắt buộc phải thực hiện.
- Chính sách cần nghiên cứu, soạn thảo kỹ lưỡng và đầy đủ, đúng đắn, thỏa mãn: có sẵn, dễ hiểu, được xác nhận, thực thi thống nhất và công bằng

Chính sách (Policies) và Luật(tiếp)

➔ Sự khác nhau giữa chính sách và luật

- Chính sách là các mục tiêu đã nêu; luật là những quy tắc bắt buộc phải theo.
- Các chính sách phản ánh các mục tiêu của chính phủ, luật pháp cung cấp khuôn khổ pháp lý và thể chế để hoàn thiện các chính sách này

Chính sách (Policies) và Luật(tiếp)

➔ Sự khác nhau giữa chính sách và luật

- Các chính sách được chính phủ đưa ra dưới dạng danh nghĩa công khai và chính phủ phải soạn thảo các dự luật và thông qua chúng để đưa các chính sách này thành hình thức cụ thể của luật
- Chính sách là những gì chính phủ dự định làm; pháp luật giúp nó thực hiện những gì nó dự định làm.



II: Luật quốc tế về ATTT

CÁC LUẬT LIÊN QUAN CỦA USA



Đạo luật Tự do Thông tin năm 1966:
Cho phép tiết lộ thông tin và tài liệu chưa được phát hành trước đây do chính phủ Hoa Kỳ kiểm soát



Đạo Luật Lạm dụng và Gian lận Máy tính năm 1986: Xác định và chính thức hóa luật để chống lại các mối đe dọa từ các hành vi và hành vi phạm tội liên quan đến máy tính.



Đạo Luật bảo mật máy tính năm 1987: Yêu cầu tất cả các hệ thống máy tính liên bang có chứa thông tin đã phân loại phải có kế hoạch bảo mật và yêu cầu đào tạo định kỳ cho tất cả các cá nhân vận hành, thiết kế hoặc quản lý các hệ thống đó



Đạo luật về trách nhiệm giải trình và cung cấp bảo hiểm y tế năm 1996 (HIPAA): Yêu cầu thực thi y tế để đảm bảo quyền riêng tư của thông tin y tế cá nhân



Gramm-Leach-Bliley (GLB) 1999 hay Đạo luật hiện đại hóa dịch vụ tài chính: Bãi bỏ các hạn chế đối với các ngân hàng liên kết với các công ty bảo hiểm và chứng khoán; có tác động đáng kể đến quyền riêng tư của thông tin cá nhân được sử dụng bởi các ngành này



Đạo luật Sarbanes-Oxley năm 2002: (còn được gọi là Đạo luật Cải cách Kế toán Công ty Đại chúng và Bảo vệ Nhà đầu tư) : Thực thi trách nhiệm giải trình đối với người điều hành tại các công ty giao dịch công khai như kế toán tài chính, CNTT, và các đơn vị liên quan của nhiều tổ chức

Các luật ATTT của Mỹ (tiếp)

- Luật xuất khẩu và chống gián điệp (hạn chế việc xuất khẩu các công nghệ và hệ thống xử lý thông tin, phòng chống gián điệp kinh tế):
 - Economic Espionage Act, 1996.
 - The Security and Freedom through Encryption Act 1999.
- Luật bản quyền Mỹ (U.S Copyright Law): điều chỉnh các vấn đề có liên quan đến xuất bản, quyền tác giả của các tài liệu, phần mềm, bao gồm cả các tài liệu số.

Các luật ATTT của Mỹ (tiếp)

- Luật tự do thông tin (Freedom of Information Act, 1966 – FOIA): các cá nhân được truy nhập các thông tin không gây tổn hại đến an ninh quốc gia.
- Một số luật pháp gần đây:
 - National Cybersecurity Protection Act (NCPA)
 - Cybersecurity Enhancement Act 2014 (CEA)
 - Federal Information System Modernization Act of 2014 (FISMA 2014)
 - Cybersecurity Workforce Assessment Act (CWWA)
 - Cybersecurity Act of 2015

Các tổ chức thực thi luật pháp

- Federal Bureau of Investigation (FBI): cục Điều tra Liên bang Hoa Kỳ.
- National Security Agency - Information Assurance Directorate (IAD): Cơ quan An ninh Quốc gia – Cục đảm bảo thông tin.
- U.S. Secret Service: Cơ quan Mật vụ Hoa Kỳ.
- Department of Homeland Security: Bộ an ninh nội địa.

Luật Quốc tế và các tổ chức pháp lý liên quan đến ATTT

- Hiện tại có rất ít Luật Quốc Tế liên quan đến vấn đề Quyền riêng tư và An toàn thông tin.
- Hội đồng châu Âu về chống tội phạm mạng (Council of Europe Convention on Cybercrime)
- Hiệp ước bảo vệ quyền sở hữu trí tuệ (Agreement on Trade-Related Aspects of Intellectual Property Rights – TRIPS).
- Digital Millennium Copyright Act (DMCA): luật bản quyền số Thiên niên kỷ.
- European Union Directive 95/46/EC.



III: Vấn đề đạo đức ATTT

Đạo đức (Ethics)

Đạo đức: Định nghĩa những hành vi mà xã hội chấp nhận được

- Đạo đức dựa trên các đặc điểm văn hóa, do đó, đạo đức giữa các quốc gia, các dân tộc trên thế giới có thể khác nhau.
- ➡ Luật được thực thi bởi các cơ quan chính quyền >< Đạo đức không được thực thi bởi các cơ quan chính quyền mà do xã hội nhìn nhận.

Đạo đức (tiếp)

- Yếu tố quan trọng nhất trong việc xây dựng nhận thức về đạo đức trong một quy mô dân số nhỏ chính là Giáo dục
 - ➔ Đạo đức và Giáo dục có mối quan hệ mật thiết với nhau.
- Một số tổ chức lớn đặt ra những bộ quy tắc đạo đức và ứng xử: ACM, SANS, ISC2, ISACA, ISSA.
- Các cá nhân, tổ chức thuộc ngành ATTT cần nỗ lực hết sức mình để ngăn chặn các hành vi vô đạo đức và bất hợp pháp dù các hành vi này có thể do thiếu hiểu biết, vô tình hay cố ý.

Sự cần thiết của đạo đức ATTT

- Thông tin nhạy cảm, hệ thống bí mật quốc gia; thông tin bí mật của cơ quan, tổ chức;... chúng có thể bị rò rỉ, đánh cắp hoặc lạm dụng, gây ảnh hưởng nghiêm trọng đến an ninh quốc gia.
- ⇒ Người làm trong lĩnh vực ATTT cần phải có hiểu biết về chính sách, pháp luật, và có thái độ, hành động đúng đắn trong khi thực thi nhiệm vụ.

Một số quy tắc ứng xử trong ATTT

- Không có bộ quy tắc ứng xử bắt buộc nào.
- Một số tổ chức nghề nghiệp ACM và ISSA hợp tác đề ra các quy tắc ứng xử trong ATTT, tuy nhiên chúng chỉ mang tính khuyến nghị chứ không bắt buộc phải thực hiện.
- Hiệp hội ATTT VN công bố bộ quy tắc ứng xử ATTT đầu năm 2015 về những điều không được làm của các thành viên hoạt động trong lĩnh vực ATTT.

Đạo đức cho người sử dụng máy tính

- Không sử dụng máy tính để làm hại người khác.
- Không sử dụng máy tính để ăn cắp thông tin của người khác.
- Không truy cập các tập tin mà không có sự cho phép của chủ sở hữu.
- Không sao chép phần mềm có bản quyền mà không có sự cho phép của tác giả.
- Luôn luôn tôn trọng luật pháp và chính sách bản quyền.
- Tôn trọng sự riêng tư của người khác, cũng giống như bạn mong đợi sự tôn trọng riêng tư từ những người khác.
- Sử dụng Internet có đạo đức.

Đạo đức cho người sử dụng máy tính (tiếp)

- Không sử dụng tài nguyên máy tính của người khác khi chưa có sự cho phép của họ.
- Khiếu nại về việc cung cấp thông tin hay các hoạt động bất hợp pháp khác, nếu biết, đến các nhà cung cấp dịch vụ Internet và các cơ quan thực thi pháp luật địa phương.
- Người sử dụng có trách nhiệm bảo vệ tài khoản và mật khẩu của họ. Không nên viết ra giấy hoặc bất cứ nơi nào khác để nhớ.
- Người dùng không nên cố ý sử dụng máy tính để truy xuất hoặc sửa đổi thông tin của người khác, ví dụ như thông tin mật khẩu, các tập tin.

Bộ quy tắc ứng xử bởi viện đạo đức mt(Mỹ)

1. Không được dùng máy tính gây phiền cho người khác
2. Không được can thiệp vào công việc máy tính của người khác
3. Không được đánh cắp các tệp dữ liệu máy tính của người khác
4. Không được dùng máy tính để ăn cắp
5. Không được dùng máy tính để tạo bằng chứng giả
6. Không được copy các phần mềm có bản quyền

Bộ quy tắc ứng xử bởi viện đạo đức mt(Mỹ)

7. Không được dùng tài nguyên máy tính của người khác khi không được phép
8. Không được lợi dụng phi pháp sản phẩm trí tuệ của người khác
9. Phải nghĩ đến những hậu quả xã hội mà chương trình máy tính của mình gây ra
10. Cần dùng máy tính theo những chuẩn mực và tôn trọng những luân thường đạo lý của con người

Ngăn chặn hành vi phi đạo đức và bất hợp pháp

- Cần phải đào tạo và giáo dục về chính sách và luật, làm các biện pháp để kiểm soát hoặc bảo vệ thông tin hệ thống
- Hành vi phi đạo đức, bất hợp pháp chia thành:
 - + Thiếu hiểu biết về luật
 - + Vi phạm không có chủ đích
 - + Vi phạm có chủ đích
- Răn đe là phương pháp tốt nhất để ngăn chặn một hoạt động bất hợp pháp. Luật pháp, các phương pháp kiểm soát kỹ thuật... là những ví dụ về các biện pháp ngăn chặn.



IV: Quản lý các cuộc điều tra trong một tổ chức

Quản lý các cuộc điều tra trong tổ chức

“Vấn đề không phải là ‘nếu’, mà là ‘khi nào’?”

- Các bước thực hiện điều tra:
 - Tài liệu chính là chìa khóa mấu chốt.
 - Digital Forensics - Điều tra số (Pháp y kỹ thuật số)

Điều tra số

- Là một nhánh của khoa học điều tra với mục đích truy tìm, phân tích các tài liệu trong thiết bị số, để tìm ra các bằng chứng số liên quan đến tội phạm.
- Điều tra những gì đã xảy ra và xảy ra như thế nào, phân tích các bằng chứng và các nguyên nhân gốc rễ
- Tìm kiếm thông tin dựa trên các chính sách hoặc luật pháp có khả năng hỗ trợ các tổ chức chống lại kẻ tình nghi.

Điều tra số (tiếp)

- 2 mục đích chính của điều tra số:
 - Điều tra các cáo buộc về lỗi kỹ thuật số.
 - Thực hiện phân tích nguyên nhân gốc rễ.
- Các phương pháp tiếp cận:
 - Protect and forget (patch and proceed)
 - Apprehend and prosecute (pursue and prosecute)

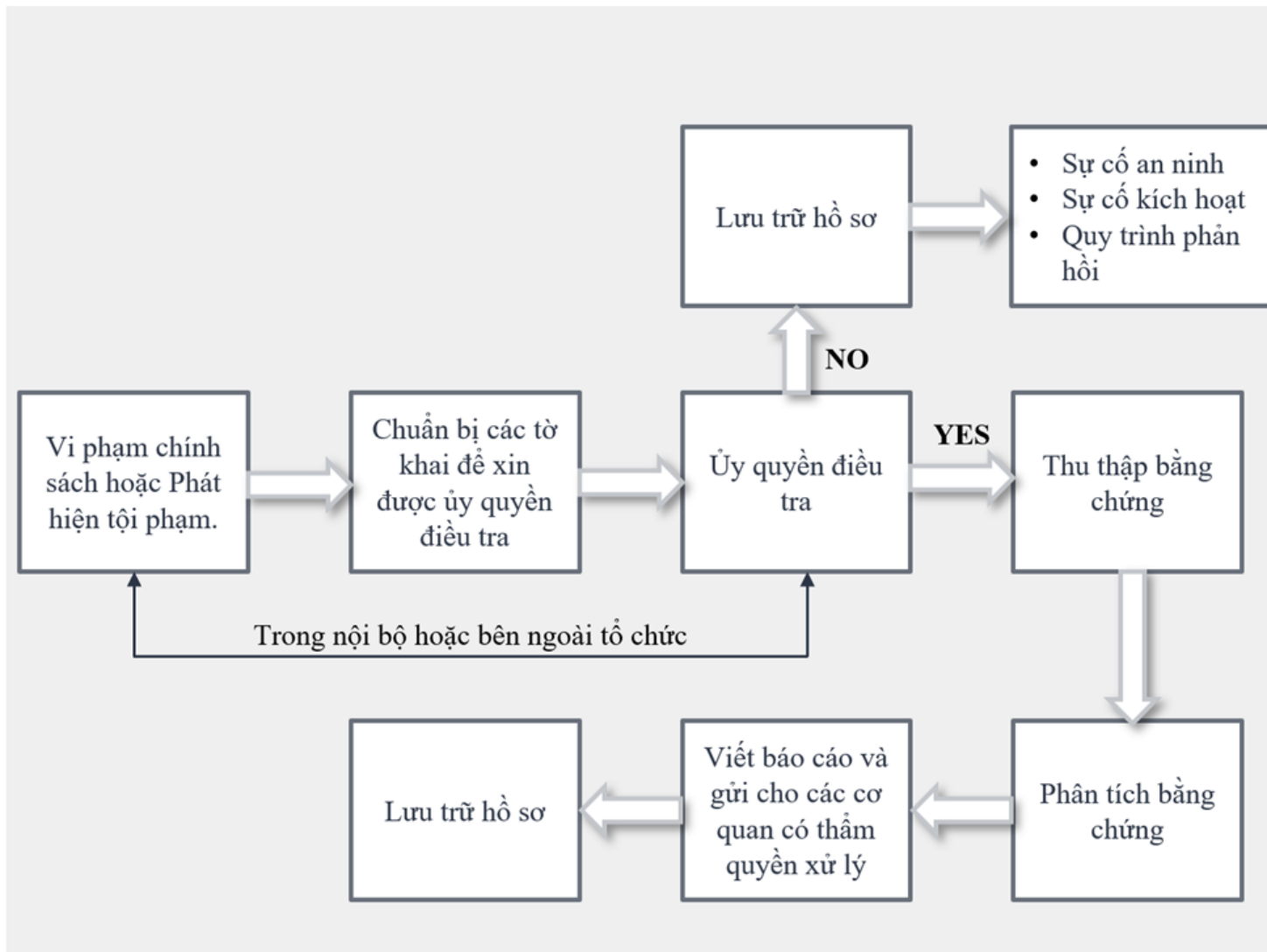
Điều tra số (tiếp)

- Các cuộc điều tra bắt đầu với một cáo buộc được đưa ra hoặc xuất hiện dấu hiệu của một sự cố.
- Nhóm pháp y yêu cầu quyền kiểm tra các phương tiện kỹ thuật số để tìm các EM (Evidentiary Material) tiềm năng:
 - Bản khai
 - Lệnh khám xét

Phương pháp Điều tra số

- Xác định các hạng mục, các tài liệu liên quan có giá trị làm bằng chứng.
- Thu thập những bằng chứng không bị thay đổi hoặc bị phá hoại.
- Thực hiện các bước để đảm bảo rằng bằng chứng luôn có thể được xác thực ở mọi bước và không thay đổi so với thời điểm bị thu giữ.
- Phân tích các dữ liệu không gặp rủi ro khi sửa đổi hoặc truy cập trái phép.
- Báo cáo các phát hiện cho cơ quan có thẩm quyền thích hợp.
- Thủ tục chứng thực

Sơ đồ Điều tra số:



THANK FOR WATCHING

Do you have any question?