* Mô hình kinh doanh là trung tâm của kế hoạch kinh doanh (business plan).
* Kế hoạch kinh doanh
  + tài liệu mô tả mô hình kinh doanh của công ty.
  + tính đến môi trường cạnh tranh.
* Mô hình kinh doanh thương mại điện tử tận dụng những phẩm chất độc đáo của Internet, Web và nền tảng di động

Canvas

**1. Phân khúc khách hàng - Customer Segment:**xác định các phân khúc khách hàng nhau mà doanh nghiệp muốn hướng tới. Nhóm khách hàng này có thể là thị trường đại chúng (mass market), thị trường ngách (niche market), thị trường hỗn hợp (multi-sided market).

**2. Mục tiêu giá trị - Value Propositions:**mô tả lại những mục tiêu giá trị mà sản phẩm/dịch vụ của doanh nghiệp đã và đang tạo cho nhóm khách hàng mục tiêu. Nói cách khác, đây là lý do mà khách hàng chọn của công ty bạn thay vì công ty của đối thủ.

**3. Các kênh truyền thông – Channels:**mô tả các kênh truyền thông và phân phối mà doanh nghiệp sử dụng để tiếp xúc với phân khúc khách hàng. Qua đó mang cho khách hàng các giá trị mục tiêu mà khách hàng mong muốn. Có thể có rất nhiều kênh phân phối khác nhau bao gồm các kênh phân phối trực tiếp (đội bán hàng trực tiếp, điểm bán hàng trực tiếp, gian hàng trên mạng…) và kênh phân phối gián tiếp (đại lý bán hàng, cửa hàng của đối tác…)

**4. Quan hệ khách hàng - Customer Relationships:**mô tả các loại quan hệ mà doanh nghiệp muốn thiết lập với các phân khúc khách hàng của mình. Làm thế nào doanh nghiệp giữ chân khách hàng cũ

hoặc thu hút khách hàng mới

**5. Dòng danh thu - Revenue Streams:** thể hiện luồng lợi nhuận doanh nghiệp thu được từ các phân khúc khách hàng của mình. Nếu khách hàng được coi là trái tim của mô hình kinh doanh thì luồng lợi nhuận được coi là các động mạch của nó. Dòng danh thu chính là ô mà các nhà [đầu tư](http://cafebiz.vn/dau-tu.html) quan tâm nhất.

**6. Nguồn lực chính - Key Resources**: mô tả các nguồn lực quan trọng nhất của doanh nghiệp để hoạt động kinh doanh có thể tồn tại. Để tạo ra được hàng hóa, thiết lập kênh truyền thông và phân phối, duy trì quan hệ khách hàng … bạn cần phải có những nguồn lực nhất định và nếu không có nguồn lực này thì bạn không thể kinh doanh được. Đây có thể là các nguồn lực vật lý (ví dụ tài nguyên môi trường), nguồn lực tri thức (bằng sáng chế), nhân lực và tài chính.

**7. Hoạt động chính - Key Activities (KA)**: mô tả các hành động quan trọng nhất mà doanh nghiệp cần duy trì để giữ được công việc kinh doanh của mình. Một cách trừu tượng, là các hành động sử dụng nguồn lực (KR) để có thể tạo ra các giá trị mục tiêu khác biệt (VP) và qua đó thu được lợi nhuận (RS). Ví dụ đối với công ty như Facebook, hoạt động chính sẽ là phát triển nền tảng và xây dựng trung tâm dữ liệu. Đối với công ty tư vấn luật, key activities là việc nghiên cứu văn bản luật và tư vấn pháp luật.

**8. Đối tác chính - Key Partnerships (KP)**: mô tả các nhà cung cấp nguồn lực và các đối tác giúp cho công việc kinh doanh được thực thi tốt và có thể phát triển. Có thể là một trong bốn loại sau : đối tác chiến lược giữa các công ty không phải là đối thủ của nhau, đối tác giữa các công ty là đối thủ của nhau để cùng nâng thị trường lên, cùng đầu tư (joint ventures) để tạo ra công việc kinh doanh mới, quan hệ mua bán để đảm bảo đầu vào cho công ty.

**9. Cơ cấu**[**chi phí**](http://cafebiz.vn/chi-phi.html)**- Cost Structure (CS)**: mô tả tất cả các chi phí cần thiết để duy trì và điều hành một công việc kinh doanh. Một số mô hình kinh doanh chú trong vào giá rất nhiều như mô hình kinh doanh vé máy bay giá rẻ của Jetstar, một số khác chú trọng tạo dựng giá trị cho người mua (ví dụ như các khách sạn 4-5 sao)… Đây cũng là nơi nhà đầu tư bỏ tiền vào.

**1 Các loại tội phạm trên mạng**

Trên mạng máy tính internet hiện nay hàng ngày có rất nhiều vấn đề tội phạm tin học đã và đang xảy ra. Có một số loại tội phạm chính sau: Gian lận trên mạng là hành vi gian lận, làm giả để thu nhập bất chính. Ví dụ sử dụng số thẻ VISA giả để mua bán trên mạng. Tấn công Cyber là một cuộc tấn công điện tử để xâm nhập trái phép trên internet vào mạng mục tiêu để làm hỏng dữ liệu, chương trình, và phần cứng của các website hoặc máy trạm.

Hackers (tin tặc): Hackers nguyên thuỷ là tiện ích trong hệ điều hành Unix giúp xây dựng Usenet, và World Wide Web... Nhưng, dần dần thuật ngữ hacker để chỉ người lập trình tìm cách xâm nhập trái phép vào các máy tính và mạng máy tính Crackers: Là người tìm cách bẻ khoá để xâm nhập trái phép vào máy tính hay các chương trình.

 Các loại tấn công trên mạng: 1> Tấn công kỹ thuật là tấn công bằng phần mềm do các chuyên gia có kiến thức hệ thông giỏi thực hiện 2> Tấn công không kỹ thuật là việc tìm cách lừa để lấy được thông tin nhạy cảm 3> Tấn công làm từ chối phục vụ (Denial-of-service (DoS) attack) là sử dụng phần mềm đặc biệt liên tục gửi đến máy tính mục tiêu làm nó bị quá tải, không thể phục vụ được 4> Phân tán cuộc tấn công làm từ chối phục vụ (Distributed denial of service (DDoS) attack) là sự tấn công làm từ chối phục vụ trong đó kẻ tấn công có quyền truy cập bất hợp pháp vào vào nhiều máy trên mạng để gửi số liệu giả đến mục tiêu 5>Virus là đoạn mã chương trình chèn vào máy chủ sau đó lây lan. Nó không chạy độc lập 6> Sâu Worm là một chương trình chạy độc lập. Sử dụng tài nguyên của máy chủ để lan truyền thông tin đi các máy khác.

Các cuộc tấn công tin tặc trên mạng ngày càng tăng trên mạng Internet và ngày càng đa dạng vi trên mạng hiện giờ là thông tin và tiền. Các nhân tố tác động đến sự ra tăng tin tặc là sự phat triển mạnh của TMĐT và nhiều lỗ hổng công nghệ của các website.

**4. Cơ chế mã hoá**

Để đảm bảo an toàn bảo mật cho các giao dịch, người ta dùng hệ thống khoá mã và kỹ thuật mã hoá cho các giao dịch TMĐT. Mã hoá là quá trình trộn văn bản với khoá mã tạo thành văn bản không thể đọc được truyền trên mạng.

Khi nhận được bản mã, phải dùng khoá mã để giải thành bản rõ. Mã hoá và giải mã gồm 4 thành phần cơ bản: 1> Văn bản rõ – plaintext 2> Văn bản đã mã – Ciphertext 3> Thuật toán mã hoá - Encryption algorithm 4> Khoá mã – Key — là khoá bí mật dùng nó để giải mã thông thường. Mã hoá là tiền đề cho sự thiết lập các vấn đề liên quan đến bảo mật và an ninh trên mạng

Có hai phương pháp mã hoá phổ biến nhất: phương pháp mã đối xứng (khoá riêng): dùng để mã và giải mã điện rõ, cả người gửi và người nhận đều sử dụng văn bản.

Mã hoá dùng khoá riêng Mã ko đối xứng (mã công cộng): sử dụng một cặp khoá: công cộng và riêng, khoá công cộng để mã hoá và khoá riêng để giải mã. Khi mã hoá người ta dùng hai khoá mã hoá riêng rẽ được sử dụng. Khoá đầu tiên được sử dụng để trộn các thông điệp sao cho nó không thể đọc được gọi là khoá công cộng. Khi giải mã các thông điệp cần một mã khoá thứ hai, mã này chỉ có người có quyền giải mã giữ hoặc nó được sử dụng chỉ bởi người nhận bức thông điệp này, khoá này gọi là khoá riêng.

Ðể thực hiện các công việc mã hoá và giải mã, cần một cơ quan trung gian giữ các khoá riêng, đề phòng trường hợp khoá này bị mất hoặc trong trường hợp cần xác định người gửi hoặc người nhận. Các công ty đưa ra các khoá mã riêng sẽ quản lý và bảo vệ các khoá này và đóng vai trò như một cơ quản xác định thẩm quyền cho các mã khoá bảo mật.

**5. Chứng thực số hoá**  Chứng thực số để xác nhận rằng người giữ các Name : “Richard” khoá công cộng và khoá riêng là ai đã đăng key-Exchange Key : ký. Cần có cơ quan trung gian để làm công Signature Key : Serial # : 29483756 việc xác thực. Chứng thực có các cấp độ khác Other Data : 10236283025273 nhau. Expires : 6/18/04 Signed : CA’s Signature Không phải tất cả các mã khoá riêng hay các chứng chỉ số hoá đều được xây dựng như nhau. Loại đơn giản nhất của giấy chứng chỉ hoá được gọi là chứng nhận Class 1, loại này có thể dễ dàng nhận khi bất kỳ người mua nào truy nhập vào WEB site của VeriSign (www.verisign.com ). Tất cả những cái mà doanh nghiệp phải làm là cung cấp tên, địa chỉ và địa chỉ e-mail, sau khi địa chỉ e-mail được kiểm tra, sẽ nhận được một giấy chứng nhận số hoá. Về mặt nào đó nó cũng giống như một thẻ đọc thư viện

Các chứng nhận Class 2 yêu cầu một sự kiểm chứng về địa chỉ vật lý của doanh nghiệp, Ðể thực hiện điều này các công ty cung cấp chứng nhận sẽ tham khảo cơ sở dữ liệu của Equifax hoặc Experian trong trường hợp đó là một người dùng cuối và Dun&Bradstreet trong trường hợp đó là một doanh nghiệp. Quá trình này giống như là một thẻ tín dụng. Mức cao nhất của một giấy chứng nhận số hoá được gọi là chứng nhận Class 3. Có thể xem nó như là một giấy phép lái xe. Ðể nhận được nó doanh nghiệp phải chứng minh chính xác mình là ai và phải là người chịu trách nhiệm. Các giấy phép lái xe thật có ảnh của người sở hữu và được in với các công nghệ đặc biệt để tránh bị làm giả. Các giấy chứng nhận Class 3 hiện chưa được chào hàng, tuy nhiên các công ty hoạt động trong lĩnh vực an toàn và bảo mật đã mường tượng ra việc sử dụng nó trong tương lai gần cho các vấn đề quan trong như việc đàm phán thuê bất động sản qua WEB hoặc vay vốn trực tuyến. Nó cũng có thể được sử dụng như là các chứng nhận định danh hợp pháp hỗ trợ việc phân phát các bản ghi tín dụng hoặc chuyển các tài liệu của toà án. Hiện tại các biểu mẫu thu nhận thông tin thanh toán trên WEB thường đạt chứng nhận an toàn và bảo mật Class 1, nhưng hiện tại một số cửa hàng trên WEB cũng đã đạt mức an toàn và bảo mật Class 2 và khách hàng cũng đã bắt đầu nhận được chúng thông qua một công nghệ được gọi là SET.

**6.  Một số giao thức bảo mật thông dụng**

a. Cơ chế bảo mật SSL (Secure Socket Layer) Về mặt lý thuyết rất nhiều công ty có thể đóng vai trò như một cơ quan chứng thực thẩm quyền. VeriSign Inc (www.verisign.com), là công ty cung cấp dịch vụ về chứng thực số dẫn đầu tại Mỹ. Công ty này sử dụng bản quyền về công nghệ từ RSA Inc. (www.rsa.com). RSA giữ đăng ký sáng chế về công nghệ mã khoá riêng/công cộng được giới thiệu vào năm 1976 củaWhitfield Diffie và Martin Hellman và nó được chuyển giao cho VeriSign vào năm 1995 cho dù các công ty khác cũng giữ quyền sử sử dụng nó. Để bảo mật, doanh nghiệp phải mua một khoá riêng từ VeriSign thu phí 349 USD/ năm cho một WEB site thương mại với một khoá bảo mật như vậy và phí để bảo dưỡng hàng năm là 249 USD, doanh nghiệp có thể mua thêm khoá bảo mật với mức giá tương đương. Sau khi máy chủ nhận được một khoá mã bảo mật, việc tiếp nhận một đơn đặt hàng trở nên đơn giản. quot;Ðiểm nổi bật của SSL ta có thể ngay lập tức tạo một trang HTML với các biểu mẫu để khách hàng cung cấp thông tin về họ trong lúc giao dịch, và đảm bảo rằng các thông tin này được bảo mật và mã hoá khi được gửi đi trên Internetquot; . Sau khi các thông tin mà khách hàng nhập vào các biểu mẫu trên trang WEB hiển thị trên trình duyệt của họ đước mã hoá với SSL nó được gửi đi trên Internet một cách an toàn. Trong thực tế khi người sử dụng truy nhập vào các trang WEB được hỗ trợ bởi SSL, họ sẽ thấy một biểu tượng như một chiếc khoá ở thanh công cụ bên dưới chương trình.

**SQL Injection** là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn lấy dữ liệu của những website không an toàn trên web, đây là một kỹ thuật tấn công rất phổ biến và sự thành công của nó cũng tương đối cao.

Đọc qua thì các bạn cũng hiểu sơ sơ rồi phải không nào, giờ mình sẽ một vài lý do đã tạo nên tên tuổi lừng lẫy của **SQL Injection**:

* Có thể gây ra những thiệt hại khổng lồ. Với SQL Injection, hacker có thể truy cập một phần hoặc toàn bộ dữ liệu trong hệ thống.
* Lỗ hổng này rất nổi tiếng, từ developer đến hacker gần như ai cũng biết. Ngoài ra, còn có 1 số tool tấn công SQL Injection cho dân “ngoại đạo”, những người không biết gì về lập trình.
* Rất nhiều ông lớn từng bị dính – Sony, Microsoft UK. Mọi vụ lùm xùm liên quan tới “lộ dữ liệu người dùng” ít nhiều đều dính dáng tới SQL Injection.

Dễ tấn công, phổ biến, gây ra hậu quả nghiêm trọng, đó là lý dó Inject (Không chỉ SQL mà OS và LDAP) nằm chễm chễ ở vị trí đầu bảng trong top 10 lỗ hỗng bảo mật của OWASP. Tất nhiên là XSS, CSRF, và không mã hoá dữ liệu cũng nằm trong list này nốt.

Cơ chế SQL Injection vô cùng đơn giản. Ta thường sử dụng câu lệnh SQL để truy cập dữ liệu.

**Cách phòng chống SQL Injection**

May thay, mặc dù SQL rất nguy hại nhưng cũng dễ phòng chống. Gần đây, hầu như chúng ta ít viết SQL thuần mà toàn sử dụng ORM (Object-Relational Mapping) framework. Các framework web này sẽ tự tạo câu lệnh SQL nên hacker cũng khó tấn công hơn.