 Khi các nhà quản trị công ty đối mặt với một vụ khủng hoảng. Chẳng hạn như sản phẩm bị thu hồi hay người lãnh đạo bị tai tiếng, thì phản ứng tự nhiên tiêu biểu của họ là giương cờ trắng đầu hàng.

Nhưng theo chuyên gia xử lý khủng hoảng Eric Dezenhall, đồng tác giả của cuốn sách mới xuất bản mang tên Kiểm soát thiệt hại: Tại sao mọi điều bạn biết về quản lý khủng hoảng đều sai (Nxb Portfolio, 2007), chiến lược phản ứng đó không đứng được khi các giám đốc phải chống đỡ những đối thủ cạnh tranh "khát máu" hoặc một công chúng khách hàng đang hoảng hốt. Trong cuộc phỏng vấn đăng trên tờ Computerworld mới đây, Eric Dezenhall trò chuyện với phóng viên Thomas Hoffman xung quanh đề tài các giám đốc công nghệ thông tin (CNTT) và các nhà lãnh đạo doanh nghiệp nên xử lý khủng hoảng như thế nào.

Một ngân hàng chẳng hạn sẽ đối phó như thế nào với một vụ rối loạn công cộng khi hệ thống máy tính của mình bị hacker đột nhập và dữ liệu tài chính của hàng chục ngàn khách hàng bị đánh cắp?

– Trước tiên hãy nhớ rằng tên gọi của trò chơi này là kiểm soát thiệt hại chứ không phải là xóa dấu vết thiệt hại. Bạn không thể đảo ngược tình hình, bạn chỉ có thể làm nhẹ tác động của thiệt hại. Chúng ta đã có những tình huống giống như thế và bạn cần phải định lượng vấn đề. Cần nhanh chóng làm rõ quy mô và mức độ của sự thiệt hại. Mọi người đều muốn biết, "Liệu mình có ổn không ?" và "Bạn đang làm gì về chuyện đó ?" Đây là hai mục tiêu sánh đôi trong việc xử lý khủng hoảng: bảo vệ quyền lợi của khách hàng và có giải pháp xử lý khủng hoảng phù hợp. Nhiều công ty cứ liên tục đưa ra những lời giải thích nhưng đối với công chúng đang hoảng loạn, giải thích là hoàn toàn vô ích.

N u nh hacker t nh p c v o h th ng d li u v b nh nh n c a m t c s y t th x l theo c ch kh c c kh ng?

– Tôi cho rằng vẫn phải áp dụng những nguyên tắc như vậy. Thông tin về tình trạng tài chính và về tình trạng sức khỏe đều là những thông tin mang tính cá nhân. Khi khủng hoảng xảy ra bạn phải đối mặt với những khách hàng đang nổi giận đến mức họ không chịu nghe những lý lẽ thông thường. Họ muốn được bảo đảm rằng sự cố đã được kiểm soát và trong tương lai sẽ không xảy ra những sự cố tương tự. Giải thích cho họ hiểu hệ thống bị đột nhập như thế nào thì cũng giống như ông thợ ống nước giải thích cho bạn vì sao ống cống nhà bạn bị tắc trong lúc bạn chỉ cần nó hoạt động.

Nhi u v kh ng ho ng trong CNTT li n quan n th i n t (e-mail)...?

– Đây là một nạn dịch. Những người không sao lưu một số e-mail nào đó thường là những người quá già đến mức không sử dụng e-mail hoặc là

những người phải trả cả trăm ngàn đô-la để dàn xếp những vụ kiện tụng vì đã không lưu lại những e-mail quan trọng.

Khi khủng hoảng xảy ra: Đừng phức tạp hóa vấn đề

Khi phải đương đầu với khủng hoảng, đôi khi những việc bạn không làm cũng quan trọng như những việc bạn làm vậy. Kinh nghiệm của các giám đốc CNTT là:

Đừng tạo ra một khoảng trống quyền lực. Bạn hay người được ủy quyền phải sẵn sàng đưa ra quyết định khi các nhân viên của bạn cố gắng xác định những biện pháp kỹ thuật cần thiết để ngăn ngừa khủng hoảng lan rộng. Đồng thời phải quy định rõ bằng cách nào và lúc nào nhân viên có thể đề đạt những ý kiến phản đối, tranh luận hoặc những vấn đề khác nữa mà họ không tự giải quyết được.

Đừng hứa hẹn những điều mà bạn không chắc rằng bạn có thể thực hiện được. Nếu bạn không thực hiện được lời hứa bạn sẽ tự làm giảm uy tín của mình và tình hình sẽ tồi tệ hơn nữa.

Dục tốc bất đạt, đừng bắt nhân viên phải thay đổi quá nhiều và quá nhanh. Nhân viên của bạn có thể chịu đựng vài tuần làm việc không ngừng nghỉ, đặc biệt là khi họ phải chạy đua với thời gian để khắc phục sự cố. Nhưng nếu như buộc họ phải thực hiện nhiều cải tiến ngay lập tức sau khi xảy ra khủng hoảng, họ có thể bị kiệt sức và chán nản.

Đừng can thiệp quá sâu. Điều quan trọng là bạn phải thể hiện tình đoàn kết với đội ngũ CNTT của mình nhưng bạn không nên dành quá nhiều thời gian để trực tiếp “tác chiến”. Thay vì vậy, hãy cân bằng thời gian cho những tập thể mà bạn phục vụ, chẳng hạn như nhân viên, đồng nghiệp, công chúng, ban lãnh đạo và tổng giám đốc điều hành.

N u nh m t ch ng tr nh qu n l t i nguy n doanh nghi p (ERP) b r i lo n ch c n ng v l m nh tr ho t ng, nh tr ng h p x y ra v i nh s n xu t s -c -la Hershey Foods, m y gi t Whirlpool v gi y th thao Nike, th c ng ty c th l m g ?

- Chúng tôi đã từng xử lý một tình huống thuộc loại đó và câu trả lời tỏ ra đã cũ: lấy tấn công để phòng ngự. Rất nhiều lần bạn phải đối mặt với những vấn đề thuộc về hạ tầng kỹ thuật của hoạt động doanh nghiệp và cách chữa trị chính là mối quan hệ giữa người và người. Hãy tiến hành một cuộc tiến công thật sự vào các đối tác đang bực mình, thể hiện cho họ thấy bạn đã làm gì để sửa chữa vấn đề và truyền tới họ một lời cam kết cá nhân bảo đảm rằng sự cố sẽ không xảy ra nữa. Bạn nên huy động toàn bộ tập thể của bạn, trên cơ sở từng cá nhân, để xoa dịu các đối tác đang nổi giận.

Nh ng c ng ty n o x l t t s c kh ng ho ng v i u g l m cho h th nh c ng?

– Tôi nghĩ phần lớn thành công tùy thuộc vào sự lãnh đạo mạnh mẽ. Nếu phải chọn giữa một kế hoạch quản lý khủng hoảng tốt và một sự lãnh đạo mạnh, tôi sẽ chọn lãnh đạo mạnh. Trường hợp của hãng hàng không JetBlue là một minh chứng đáng chú ý.

T ng gi m c JetBlue l David Neeleman l m th n o?

– Ông ta đã làm những việc cụ thể. Khi các chuyến bay bị hủy, bị hoãn, ông ấy không chỉ xin lỗi hành khách ; ông ta đưa ra một chương trình bồi hoàn tiền vé. Họ đã công bố một danh sách các quyền của khách hàng, và đưa ra một bản cam kết đặc biệt về các hành động của hãng hàng không. Sau đó, ông ta không chỉ lúc nào cũng có mặt mà còn tỏ ra mạnh mẽ. Cái mà chúng ta muốn thấy ở người lãnh đạo là một con người đầy bản lĩnh trong một tình huống nhất định. Một người lãnh đạo luôn xun xoe, bợ đỡ, chiều ý khách hàng không phải là điều mà mọi người muốn thấy. Năm ngoái khi tập đoàn máy tính Hewlett-Packard (HP) phải đương đầu với vụ tai tiếng nghe lén và theo dõi các quản trị viên, Tổng giám đốc HP là Mark Hurd đã không xin lỗi khách hàng mà tỏ ra có bản lĩnh rất cao. Ông nói: “HP là một công ty rất mạnh và chúng tôi sẽ ra khỏi tình trạng này”. Và họ đã làm đúng như vậy.

Trong qu n l kh ng ho ng, c n c ph ng di n n o kh ng n n coi nh kh ng?

– Chúng tôi tin rằng đa số các xung đột đều liên quan đến vấn đề truyền thông. Cách xử lý khủng hoảng do truyền thông sai lệch thì khác với cách xử lý một vấn đề mà một đối thủ xấu bụng cố tình dựng ra để khai thác chỗ yếu của bạn. Mọi người cần nghĩ về bản chất của hành vi đối nghịch nhiều hơn là chúng tồn tại.

B y ph n c a k ho ch ng ph v i kh ng ho ng

• Kịch bản: Chọn ra những vụ việc có tính chất đại diện cho những vụ khủng hoảng khác nhau mà bạn có thể gặp phải, rồi tóm tắt những chiến lược, chiến thuật căn bản nhằm xử lý chúng.

• Đội ngũ: Xác định phòng ban nào đóng vai trò gì, nêu tên một số cán bộ đặc biệt sẽ là thành viên của đội ngũ ứng cứu và hỗ trợ. Bên ngoài công ty, xác định các nhà cung cấp chủ yếu, các nhóm dịch vụ có thể đóng vai trò cần thiết trong thời gian khủng hoảng.

• Thông tin: Bổ nhiệm một lãnh đạo về truyền thông của công ty để thu thập tiếng nói của mọi người trong những lúc khẩn cấp. Bảo đảm rằng mỗi thành viên của đội ứng cứu đều có một danh sách những người cần liên hệ, các số điện thoại hội nghị, các địa chỉ mạng nội bộ để huy

động sự cộng tác từ nhiều địa điểm khác nhau. Trong danh sách này phải có số điện thoại nhà riêng, địa chỉ e-mail cá nhân (không qua máy chủ e-mail của công ty), số điện thoại di động của mọi thành viên đội ứng cứu và hỗ trợ.

• Trách nhiệm: Soạn thảo chi tiết quyền hạn và trách nhiệm của các thành viên đội ứng cứu và hỗ trợ để họ có thể bắt tay ngay vào việc mà không cần phải chờ sự phê duyệt của cấp trên. Hãy nghĩ về các vai trò trong từng lớp hoạt động – chẳng hạn như thông tin cho khách hàng, thông tin nội bộ, thông tin cho đối tác, thông tin cho báo chí... Bảo đảm bao hàm những người theo dõi thu chi và ghi chép những phản ứng. Phải đưa ra các hướng dẫn xác định rõ các giá trị có tác dụng dẫn dắt sự ứng phó. Ví dụ, đối với công ty này thì đưa thông tin chính xác đến khách hàng càng nhanh càng tốt có thể là nguyên tắc tối hậu, trong khi đối với một công ty khác thì an toàn là mối quan tâm hàng đầu.

• Giữ an toàn: Hãy lưu ý cất giữ bằng cách nào và ở đâu kế hoạch và các tài liệu phụ trợ sao cho bảo đảm được sự an toàn và việc tiếp cận trong tất cả các tình huống có thể xảy ra. Một số công ty lưu giữ nhiều bản sao tài liệu trên những phương tiện lưu trữ khác nhau tại nhiều địa điểm.

• Quản lý: Bổ nhiệm một người nào đó quản lý tài liệu. Việc này bao gồm cả cập nhật kế hoạch và huấn luyện các thành viên mới của đội ứng cứu khi công ty nào cũng thường xuyên thay đổi nhân sự; tổ chức các cuộc tập luyện, kiểm tra, mô phỏng sự cố, và cải tiến kế hoạch dựa trên những kinh nghiệm khi sự kiện xảy ra.

• Kiểm tra: Hãy kiểm tra kế hoạch của bạn. Bắt đầu bằng việc làm thử toàn bộ kế hoạch để xem có vấn đề gì nổi cộm lên. Sau đó mô phỏng một sự cố thực, xem thử kế hoạch hoạt động như thế nào, rút kinh nghiệm và điều chỉnh kế hoạch cho sát thực tế.

(Theo TBVTSG)