Thông tin tống tiền 43 Tống tiền thông tin xảy ra khi kẻ tấn công hoặc người trong cuộc đáng tin cậy đánh cắp thông tin từ hệ thống máy tính và yêu cầu bồi thường cho việc trả lại thông tin hoặc thỏa thuận không tiết lộ thông tin đó. Tống tiền là phổ biến trong hành vi trộm cắp số thẻ tín dụng. Ví dụ, nhà bán lẻ dựa trên web CD Universe là nạn nhân của hành vi trộm cắp các tệp dữ liệu có chứa thông tin thẻ tín dụng của khách hàng. Thủ phạm là một hacker người Nga tên Maxus, kẻ đã tấn công nhà cung cấp trực tuyến và đánh cắp vài trăm nghìn số thẻ tín dụng. Khi công ty từ chối trả khoản tiền tống tiền 100,000 đô la, anh ta đã đăng số thẻ lên một trang web, cung cấp chúng cho cộng đồng tội phạm. Trang web của anh ấy trở nên phổ biến đến mức anh ấy phải hạn chế quyền truy cập.

Lỗi hoặc lỗi phần mềm kỹ thuật Một lượng lớn mã máy tính được viết, gỡ lỗi, xuất bản và bán trước khi tất cả các lỗi của chúng được phát hiện và giải quyết. Đôi khi, sự kết hợp của một số phần mềm và phần cứng nhất định cho thấy các lỗi mới. Những thất bại này bao gồm từ lỗi đến các điều kiện thất bại chưa được kiểm tra. Đôi khi những lỗi này không phải là lỗi, mà là các phím tắt có mục đích do các lập trình viên để lại vì những lý do lành tính hoặc ác ý. Nói chung, các tuyến truy cập phím tắt vào các chương trình vượt qua kiểm tra bảo mật được gọi là cửa bẫy và có thể gây ra vi phạm bảo mật nghiêm trọng. Lỗi phần mềm phổ biến đến mức toàn bộ các trang Web được dành riêng để ghi lại chúng. Trong số những thứ thường được sử dụng nhất là Bugtraq, được tìm thấy tại www.securityfocus.com, cung cấp thông tin cập nhật từng phút về các lỗ hổng bảo mật mới nhất, cũng như một kho lưu trữ rất kỹ lưỡng các lỗi trong quá khứ. Ngoài các mối đe dọa được đề cập ở trên, chính sách hoặc kế hoạch tổ chức còn thiếu, không đầy đủ hoặc không đầy đủ; kiểm soát thiếu, không rõ ràng hoặc không đầy đủ; phá hoại hoặc phá hoại; và sự lỗi thời về công nghệ phải được xem xét