مورد کاوی

مقاله این بخش:

آقای رئیس فکر می‌کنم کسی اطلاعات مشتریانمان را به سرقت برده است

گروه مترجمان میثاق مدیران
info@MIsaqModiran.com

آقای رئیس فکر می‌کنم کسی اطلاعات مشتریانمان را به سرقت برده است

شرکت فلایتون الکترونیک دریافته که امنیت داده ها و اطلاعات مشتریان به خطر افتاده است و به همین دلیل این شرکت با تصمیماتی دشوار دربارهٔ آنچه که باید در آینده اتخاذ کند، مواجه شده است

نویسنده: اریک مک نالتی

گروه مترجمان میثاق مدیران
info@MisaqModiran.com

هاروارد بیزینس ریویو، سپتامبر ۲۰۰۷

مقدمه

در این مقاله برت فلایتون مشکلی را که برای شرکتش پیش آمده است مبنی بر اینکه کسی اطلاعات مشتریانشان را به سرقت برده، مطرح می کند و در خلال گزارش سه تن از کارشناسان نظرات خود را در این باره ارائه می کنند.

برت فلایتون[1] مدیر عامل شرکت فلایتون الکترونیک با خواندن گزارشی که رییس بخش امنیتی شرکت بر روی میزش گذارده بود، به شدت حیرت زده شد. او که سرش را در بین دو دستش گرفته بود هیچ شباهتی به پدرش نداشت که ۲۵ سال پیش شرکت استریو و دوربین فلایتون را تأسیس کرده بود.

این گزارش امنیتی ساعت ۹ شب گذشته در حالی که برت تازه از یک سفر کاری بازگشته در اختیار وی قرار گرفته بود. او تازه مجلهٔ اخبار الکترونیکی را باز کرده بود که تلفن همراهش زنگ خورد. پشت خط، لاری بنسون[2] معاون پیشگیری از آسیب شرکت بود.

لاری که قبلاً کارآگاه پلیس در شیکاگو بود و از سه سال پیش مسئولیت امنیتی شرکت را بر عهده گرفته بود، به برت گفت: "برت، ما مشکلی داریم. این مشکل، سرقت اطلاعات است." ضمنا لاری سابقهٔ درخشانی در کاهش سرقت های اطلاعاتی و الکترونیکی و توان بالایی در ایجاد روابط مولد با مدارس، گروه های اجتماعی و نیروی انتظامی داشت.

برت پرسید: "چه نوع مشکلی؟" صدای برت همچون همیشه بسیار آرام بود و او مطمئن بود که کسی نمی تواند به این راحتی برای او مشکل ایجاد کند.

لاری در پاسخ گفت: "من هنوز خیلی مطمئن نیستم. من با بانک یونیون سنچری[3] تماس گرفتم. آنها به طور مرتب حساب‌های مجعول را بررسی می‌کنند و به ما می گویند که چه میزان از خرید مشتریان، از طریق کارت های غیرقانونی یا جعلی صورت گرفته است. آنان اطلاعات بیشتری در اختیار من قرار نداده اند که البته من هنوز از صحت و سقم آنها مطمئن نیستم. این اطلاعات یا اصلاً مهم نیستند یا اهمیت حیاتی برای ما دارند."

برت داستانی را به خاطر آورد که در یک مجله خوانده بود. این داستان در مورد سرقت تعدادی لپ تاپ بود که اطلاعات موجود در آنها نیز به سرقت رفته بود. همچنین داستان هک شدن اطلاعات شرکت ئی بی[4] و دیگر ارایه کنندگان بزرگ خدمات الکترونیکی را به خاطر آورد. شرکت او یک شرکت بزرگ و زنجیره ای منطقهای با ۳۲ فروشگاه در شش ایالت بود. همچنین این شرکت از خدمات الکترونیکی بسیار پر قدرتی بهره مند بود. به نظر می رسید شرکت فلایتون الکترونیک باید هدفی سخت و دشوار برای سرقت اطلاعات مشتریان باشد. اما آیا واقعاً چنین بود.

1.Brett Flayton
2.Laurie Benson
3.Union Century Bank

4.eBay

"لاری، فکر می کنم درست منظور تو را متوجه نشدم. مردم از کارت های سرقت شده در فروشگاه های ما استفاده می‌کنند؟ فروشندگان ما، کارت های آنان را به درستی چک نکرده اند؟"

لاری گفت: "نه منظورم این نبود. در واقع، به نظر می رسد که اطلاعات مشتریان ما به بیرون از شرکت درز کرده است."

قلمرویی جدید

برت وقتی صبح روز بعد به شرکتش رفت، شروع به بررسی این موضوع و موارد مشابه در اینترنت کرد. ظاهراً سرقت داده‌ها و اطلاعات رایج شده بود و به طرق گوناگونی از شرکت‌ها سرقت می شود. سارقان اقدام به سرقت اطلاعات کارت های اعتباری مشتریان، شماره یا کُد تأمین اجتماعی، اطلاعات حساب های بانکی و حتی آدرس پست الکترونیک آنان می کنند. به نظر می رسد بازار سیاهی برای هر نوع اطلاعات ایجاد شده است. او دریافت که مجرمان بسیار زیرک‌تر از قبل شده اند و دیگر هیچ کس از فعالیت های آنان مصون نیست. این در حالی بود که به تازگی فلایتون پول و زمان زیادی را صرف روش های نوین پرداخت از طریق کارت‌های اعتباری و بکارگیری استانداردهای مصونیت اطلاعات و داده ها کرده بود.

لاری در حالی که سکوت کرده بود، در مقابل برت نشسته بود. او قبلاً رخ دادن چنین سرقتی را پیش بینی کرده بود اما آن را حوزه و قلمرویی کاملاً جدید میدانست. در واقع تمام تجربهٔ حرفه ای او مربوط به سرقت دارایی های فیزیکی بود. در این مورد، برخی افراد به شکلی کاملاً غیرقانونی به اطلاعات دست یافته بودند اما عملاً صحنهٔ جرمی وجود نداشت که بتوان سرنخی را در آن پیدا کرد.

تجزیه و تحلیل معمول بانک یونیون سنچری در مورد کارت‌های اعتباری جعلی، نشان می داد که ۱۵ درصد خریدهای صورت گرفته از فروشگاه های شرکت فلایتون به این صورت بوده اند - این رقم یعنی استفادهٔ ۱۵۰۰ نفر یا ۱۰۰۰۰ حساب. این رقمی بسیار بالا در قبال بررسی های معمولی توسط این بانک بود. یونیون سنچری شروع به مطلع ساختن دیگر بانک ها و همچنین شرکت های صادرکنندهٔ ویزا کارت[5] و مَستر کارت[6] کرد تا ببیند آیا آنها نیز دچار مشکلات مشابهی شده اند یا خیر.

برت از لاری پرسید: "آیا ما نباید خودمان متوجه موضوع می شدیم؟ ما گزارش های منظمی را از بانک دریافت می‌کنیم."

لاری در پاسخ گفت: "الزاماً نه. ما فقط از خرید با کارت‌های جعلی مطلع می شدیم. اما الان چنین اتفاقی رخ نداده است. خریدها قانونی هستند اما از اطلاعات حساب ها در جای دیگری و به شکلی غیر قانونی استفاده شده است. ما نتوانسته بودیم این مشکل را مشخص کنیم تا این که یونیون سنچری به شکلی کاملاً اتفاقی این موضوع را بررسی و از آن مطلع شد. ۱۵۰۰ حساب یعنی یک کوه بزرگ یخ!"

برت که حالا آرام آرام متوجه مشکل شده بود، پرسید: "توان امکانات امنیتی ما چقدر است؟" وی در حالی این سئوال را کرد که متعجب شده بود که چرا سیستم های امنیتی فاقد کفایت لازم برای شناسایی این معضل بودند.

لاری پاسخ داد "من مطمئن نیستم که توان آنها چقدر است. واقعاً متأسفم. دارندگان کارت های اعتباری مورد حمایت بانک قرار دارند اما ما نمی توانیم به چنین چیزی استناد کنیم."

برت که گویی با معمایی پیچیده مواجه شده بود، دوباره گفت: "اصلاً چرا باید مشتریان را مطلع کنیم؟ آیا بانک قبلاً به مشتریانش نگفته که حساب هایشان به خطر افتاده اند؟"

لاری توضیح داد: "موضوع اینقدرها هم ساده نیست. برخی بانک ها دارای ابزارهای پیشرفتهٔ آنالیز هستند تا بتوانند الگوهای نامعمول را سریعاً شناسایی کنند اما این روشی مبهم است. اغلب بانک ها تنها مادامی به یافتن یک مشکل می پردازند که پول یک کارت اعتباری پرداخت نشده باشد. آنها معمولاً شرایط را تنها زمانی مورد تجزیه و تحلیل قرار می دهند که مشکلی بروز کرده باشد. اگر دارندگان کارت های اعتباری توجه کافی به صورت حساب هایشان نداشته باشند، چندین ماه طول می کشد تا این بدهی مورد بررسی قرار بگیرد و

تجزیه و تحلیل معمول بانک یونیون سنچری در مورد کارت‌های اعتباری جعلی، نشان می داد که ۱۵ درصد خریدهای صورت گرفته از فروشگاه های شرکت فلایتون به این صورت بوده اند - این رقم یعنی استفادهٔ ۱۵۰۰ نفر یا ۱۰۰۰۰ حساب. این رقمی بسیار بالا در قبال بررسی های معمولی توسط این بانک بود.

5.Visa Card
6.Master Card

حساب آنها مسدود شود. آن طور که من از بانک ها فهمیده‌ام، هشدار به مشتریان در این مورد که ممکن است که اطلاعات آنها به سرقت بروند، بهترین روش برای شناسایی زود هنگام چنین مسایلی است."

لاری خیلی زود دفتر برت را ترک کرد و تمام ساعات قبل از ظهر را به توجیه مدیران و تشریح احتمال آسیب پذیری زنجیرهٔ اطلاعاتی شرکت اختصاص داد. این زنجیرهٔ اطلاعاتی خودش ساختاری ساده داشت اما شناسایی نقاط ضعف آن، کار چندان ساده ای هم نبود. در ثبت های نقدی، مشتری کارت اعتباری خود را ارایه می کرد و آن را بر روی کارت خوان می کشید. اطلاعات کارت و مشخصات محصولات خریداری شده، برای تأیید یا عدم تأیید به بانک ارسال می‌شدند. همهٔ این کارها در چند ثانیه انجام میشوند. اطلاعات معامله در رایانه های شرکت ثبت و در گزارش های مختلف مالی درج می شدند. شمارهٔ کارت های اعتباری در سیستم شرکت ثبت و ذخیره نمی شدند. اتفاقاً لاری با همین بخش سیستم مشکل داشت. آیا این امکان وجود داشت که کارت خوان ها هک شوند؟ آیا ممکن بود خطوط ارتباطی میان شرکت و بانک ردیابی شوند؟ آیا اطلاعات ذخیره شده، ایمن بودند؟ آیا این امکان وجود داشت که کسی کُدی را وارد کند تا اطلاعات خاصی را به رایانه ای دور دست یا حتی رایانه ای در همان نزدیکی ها منتقل کند؟ آیا ممکن بود کسی در داخل شرکت این کار را انجام داده باشد؟ آیا ممکن بود این کار کسی باشد که به تازگی از شرکت اخراج شده است؟

لاری مجدداً به دفتر برت بازگشت و با این سؤال مواجه شد: "باید این موضوع را نیز در نظر داشت که شاید این اتفاق از سر اشتباهی سهوی رخ داده باشد. مثلاً ممکن است یکی از کارکنان از روی ندانم کاری فایل ها را در اختیار دیگران گذاشته باشد؟"

لاری گفت: "خُب این هم ممکن است ولی من اعتقاد چندانی به آن ندارم."

برت دوباره پرسید: "آیا ممکن نیست این موضوعی اتفاقی و همهٔ ۱۵۰۰ مشتری ما جزء افراد بد اقبال بوده اند؟"

لاری اندکی فکر کرد و بعد گفت: "هر چیزی ممکن است. من باید اطلاعات بیشتری به دست آورم. بانک مرا به سازمان اطلاعات و امنیت[7] معرفی کرده است. این سازمان در حال بررسی این موضوع است زیرا ظاهراً این اتفاق برای حساب‌های چند بانک دیگر نیز رخ داده است. همکاری و اعلام یافته های دیگر بانک ها به یونیون سنچری چند روزی طول خواهد کشید. برای الان، سازمان اطلاعات و امنیت توصیه می کند که ما پیشینهٔ همهٔ کسانی را به آنها ارایه کنیم که می توانسته اند به اطلاعات حساب ها دسترسی داشته باشند

حتی کسانی که قبلاً برای ما کار می کرده اند. ما باید ...ایل‌های پرسنلی و همهٔ کسانی را که ممکن است در یک سال گذشته اخراج کرده باشیم، در اختیار آنها قرار دهیم."

برت در پاسخ گفت: "مطمئنم که قبلاً سرگئی این کار را انجام داده است." برت مطمئن بود که سرگئی کیل[8] که مدیر بخش اطلاعات بود، چنین اطلاعاتی را در اختیار داشته است. برت از جایش برخاست و از پنجرهٔ اطاقش به حدود ۳۰۰ خودرویی نگاه کرد که در پارکینگ شرکت متوقف بودند. او با خود می اندیشید که صاحبان هر یک از این خودروها و کارکنانی که در سایر فروشگاه ها برای او کار می کردند، می‌توانسته اند مرتکب چنین عملی شوند. او به لاری گفت: "سازمان اطلاعات و امنیت گفته است که ما چه کارهای دیگری باید انجام دهیم؟"

لاری توضیح داد: "نخست به ما گفته اند این موضوع را حتی‌المقدور مخفی نگاه داریم تا آنها بتوانند تصویری کامل از وضعیت به عمل آمده ترسیم کنند. اما حالا که بقیهٔ بانک ها هم متوجه موضوع شدهاند، خواه ناخواه به دنبال مقابله با کارت های جعلی و حتی جمع آوری آنها خواهند بود. با این وجود، مقامات مسئول خواهان فرصت بیشتری برای تکمیل تحقیقاتشان هستند. همهٔ ما امیدواریم که آنها به نتایجی رضایت بخش دست یابند. اگرچه سازمان اطلاعات و امنیت رهبری این کار را بر عهده گرفته است اما آنها انتظار دارند واحدهای ایالتی و محلی مقابله با جعل اسناد نیز در این راه به آنها ملحق شوند."

برت گفت "اما وضعیت مشتریان ما چه میشود؟ ما نمی‌توانیم آگاهانه اجازه دهیم از کارت ها و حساب های آنها سوء استفاده شود. کسب و کار ما فقط و فقط مبتنی بر اعتماد دو جانبه است. شهرت و اعتماد، بزرگ ترین مزیت رقابتی ما است. من نمی توانم در حالی در چشمان مشتریانم نگاه کنم که می خواهم موضوعی به این مهمی را از آنها پنهان کنم."

7.Secret Service
8.Sergei Keil

لاری در پاسخ گفت: "این موضوع مهمی است ولی در جریان باشید که قرار نیست مشتریان در این زمینه هزینه ای بپردازند. تمامی هزینه های آنها پوشش داده خواهد شد. ما باید این پول را از آن خلافکارانی بگیریم که دست به ارتکاب چنین جرمی زده اند.

دفاعیات محدود

برت نمی توانست برای دستیابی به پاسخ سوالاتش بنشیند و دست روی دست بگذارد. او خیلی زود به جلسه اش پایان داد، ملاقات ها و جلسات بعدی خود را لغو و تمام انرژی خویش را صرف یافتن سرگئی کرد. او با گوش دادن به صدای انگشتانی که مدام کلیدهای مختلف روی صفحه کلید رایانه‌ها را می فشردند و کشوهای کمدها و فایل هایی که مرتباً باز و بسته می شدند، مرتباً به این موضوع فکر می کرد که هر یک از کارکنانش در طول روز چقدر اطلاعات به دست می آورند، چقدر اطلاعات ذخیره و چقدر اطلاعات منتقل می کنند.

وقتی برت به مقابل در اطاق سرگئی رسید، دید که او در حال صحبت با تلفنش بود. سرگئی آشفته به نظر می رسید. برت به او گفت: "اکنون چقدر از شرایط پیش آمده مطلع هستیم؟"

سرگئی در پاسخ برت گفت: "ما هنوز تلاش می کنیم تا ببینیم واقعاً چه اتفاقی رخ داده است."

برت با کمی عصبانیت گفت: "اما ما مطمئن هستیم که سیستم‌های مصونیت اطلاعاتمان به ویژه سیستم PCI خوب کار می کنند، درست است؟"

سرگئی گفت: "البته این سیستم خوبی است اما به هر حال ما هر روز با فن آوری های تازه ای مواجه هستیم. من سه یا چهار طرح را که در دست اجرا هستند، مورد بررسی قرار داده‌ام. در آنها از فن آوری های نوینی استفاده شده که حتی سیستم های پیشرفتهٔ شرکت ما نیز قادر نبوده اند به طور کامل از اطلاعات موجود در آنها محافظت کنند."

برت که کمی حیرت زده شده بود، با صدایی کمی لرزان پرسید: "یعنی می خواهی بگویی آنها به طور کامل از اطلاعات ما مراقبت نکرده اند."

سرگئی گفت: "آنها فقط ۷۵ درصد نیازهای امنیتی را تامین می کنند. البته نباید این نکته را فراموش کنیم که این رقم به مراتب بهتر از میانگین رایج در میان دیگر رقبای ما است." این پاسخی توجیه کننده اما صادقانه بود.

این بار برت پرسید: "ما چگونه می توانیم از شر این معضل رها شویم؟" او می دانست سیستم امنیتی به کار گرفته شده که مورد استفادهٔ اکثر شرکت های فعال در این صنعت است، نیازمند بررسی مستمر توسط متخصصان بیرون از سازمان است تا تضمین شود که سیستم کارآیی خود را حفظ کرده است ضمن این که در صورت بروز یا رؤیت اشکالی، شرکت ارایه کنندهٔ این سیستم امنیتی مسئول پرداخت جریمه است.

سرگئی گفت: "آنها هر روز سیستم ما را چک نمی کنند."

ارزشهای اصلی و محوری در خطر

بر روی میز برت، صدها عکس وجود داشت که با دوربین‌های ساخت فلایتون گرفته شده بودند. عکس های متعلق به مراسم عروسی، تعطیلات، فارغ التحصیلی، غروب خورشید، نوزادان خندان و غیره که همگی توسط مشتریان برای شرکت ارسال شده بود. برخی از این عکس ها به صورت تابلو بر روی دیوارهای فروشگاه های فلایتون نصب شده بود و به کارکنان یادآوری می کردند که مشتریان فقط کسانی نیستند که محصولات شرکت را می خرند بلکه به نوعی از زحمات آنان قدردانی می کنند. یکی از این تصاویر که در نزدیکی در اطاق برت نصب شده بود، عکس پدرش بود که او را در حال ارایهٔ یک چک نقدی به یک انجمن خیریه نشان می داد.

وقتی برت به عکس ها نگاه میکرد، باور نمی کرد که کسب و کارش با چنین شتابی رشد کرده باشد. برت پس از آنکه پدرش بازنشسته شد، جای او را گرفت تا بلندپروازی هایش را ادامه دهد. او از چند سال قبل به دنبال سرمایه گذاری های خصوصی بود و البته می دانست که باید سود خوبی را عاید این نوع

او فکر می کرد که آیا نیازی بوده که زیرساختارهای شرکتش را تغییر دهد و آن را به کسب و کاری بزرگ تر تبدیل سازد؟ آیا شرکت نیازمند توسعهٔ توانایی هایش و افزایش کارکنانش بود؟ آیا با این همه سرمایه گذاری برای توسعهٔ شرکت و در عوض عدم سرمایه گذاری کافی در زمینهٔ سیستم‌های امنیتی، فلایتون را آسیب پذیر نکرده بود؟

سرمایه گذاران کند. او یک استراتژی تهاجمی را اتخاذ کرده و مطمئن بود که این استراتژی با موفقیت توام خواهد بود. حالا او فکر می کرد که آیا نیازی بوده که زیرساختارهای شرکتش را تغییر دهد و آن را به کسب و کاری بزرگ تر تبدیل سازد؟ آیا شرکت نیازمند توسعهٔ توانایی هایش و افزایش کارکنانش بود؟ آیا با این همه سرمایه گذاری برای توسعهٔ شرکت و در عوض عدم سرمایه گذاری کافی در زمینهٔ سیستم‌های امنیتی، فلایتون را آسیب پذیر نکرده بود؟ آیا او سرعت و فشاری بیش از حد را به شرکت وارد ساخته بود؟

در بطن سرقت اطلاعات

تا پایان روز، برت تیم مدیریت ارشد را خبر کرد تا به ارزیابی یک طرح بحران بپردازند. همه چیز ناگوارتر و تلخ تر از صبح شده بود.

لاری به تیم مدیریت اطلاع داد که به کمک اطلاعات جدید به دست آمده از سایر بانک ها، تعداد حساب های سوءاستفاده شده، افزایش یافته است. هنوز رقم نهایی مشخص نشده بود اما مسلماً بیشتر از ۱۵۰۰ مورد قبلی بود.

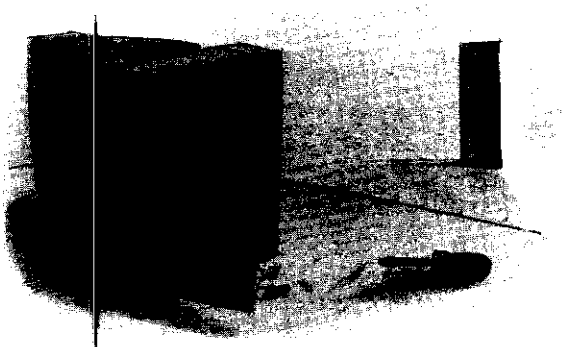
سرگئی یافته ای تلخ تر را اعلام کرد - سیستمی که از آن به عنوان سیستم بی سیم کنترل موجودی کالاها استفاده میشد از کار افتاده است و با توجه به اینکه این سیستم مستقیماً از فروشگاه ها به مرکز توزیع و از آنجا به عرضه کنندگان متصل است و نقش بسزایی در کاهش حجم نگهداری کالاها در انبار، پر بودن همیشگی قفسه ها در فروشگاه ها، کاهش هزینه‌ها و به حداقل رساندن ضرر داشته است، احتمالاً باعث درز اطلاعات داخلی شرکت به بیرون شده است.

سرگئی اظهار داشت: "همهٔ آنچه که هکر نیاز داشته، تجهیزات خوب و انگیزه های بد است. البته او باید فردی باشد که به یکی از فروشگاه های ما نزدیک است زیرا طیف درز اطلاعات بسیار محدود است." او کمی مکث کرد تا شاهد واکنش همکارانش باشد. سپس ادامه داد: "ما در تلاش هستیم تا هر چه سریع تر ایراد این سیستم رفع شود و فعالیت خود را از سر بگیرد."

لاری پرسید: "چگونه در همان مراحل نخست، این سیستم حفاظتی از کار افتاده است؟"

سرگئی در پاسخ گفت: "جواب این پاسخ تقریباً غیرممکن است. این سیستم می توانسته هم عمدی و هم اتفاقی دچار مشکل شده باشد. این سیستمی نسبتاً جدید است و چون هنوز ما آشنایی کامل با آن نداریم، با چنین مشکلاتی مواجه شده‌ایم."

برت نگاهی به بن فرایدمن[9] مدیر منابع انسانی انداخت که پرونده های عده ای از کارکنان را با خود آورده بود. فرایدمن در حالی که پرونده ها را یک به یک نشان می داد، اظهار داشت:



"پنج نفر شرکت را ترک کرده اند که همهٔ آنها قبلاً با این سیستم کار کرده اند. دو نفر استعفا داده اند، یک نفر برای ادامه تحصیل به دانشگاه بازگشته، یک نفر به دلیل مثبت اعلام شدن تست اعتیادش اخراج شده و عذر نفر آخر هم به دلیل دانلود کردن مطالب نامناسب به کمک سیستم های رایانه‌ای شرکت، خواسته شده است." او کمی مکث کرد و سپس دو پرونده را مقابل برت گذارد.

برت در حالی که به مدیر روابط عمومی یعنی سالی او کونور[10] نگاه می کرد، گفت: "خوب ما با دو مظنون مواجهیم." اوایل صبح، اوکونور یادداشتی را به برت داده بود که سه گزینهٔ مربوط به بخش ارتباطات در آن درج شده بود. یکی از این گزینه ها برگزاری یک کنفرانس مطبوعاتی بود که باعث می شد فلایتون دست پیش را بگیرد و اتفاقاً برت نیز آن را بهترین رویکرد می دانست. او علاقه ای به رویکرد دوم سالی نداشت یعنی ارسال نامه برای مشتریان و مطلع ساختن آنها از وضعیت به وجود آمده. او معتقد بود که این کار به جای ایجاد اطمینان در مشتریان باعث اضطراب آنها خواهد شد و می تواند نشانگر آن باشد که فلایتون قصد دارد چیزی را از مشتریانش مخفی کند. گزینهٔ نهایی، انجام ندادن هیچ کاری تا زمانی که سازمان اطلاعات و امنیت موضوع را علنی سازد بود و این آسان ترین راه در کوتاه مدت بود زیرا توپ تصمیم‌گیری را به سوی مدیران دیگران می انداخت.

دارل هانتینگتون[11] که مدت ها مشاور بیرونی شرکت بود و شب قبل از موضوع مطلع شده بود، از روی صندلیش برخاست و گفت: "اجازه دهید چند نکته را خاطرنشان سازم. نخست، ما هنوز هیچ دلیل مستحکمی نداریم. همهٔ شواهد به صورت مشروط هستند. از نظر من و با توجه به تجارب گذشته ام، مشخص است اولین کسی که موضوع را نزد افکار عمومی مطرح کند، به عنوان گناهکار تلقی شده و از او شکایت خواهد شد."

فرانک آردیتو[12] مدیر مالی شرکت پرسید: "چه کسی می خواهد از ما شکایت کند. هیچ یک از مشتریان متحمل

9.Bon Friedman
10.Connor'Sally O

11.Darrell Huntington
12.Frank Ardito

ضرر مالی نخواهند شد. بانک از آنها حمایت خواهد کرد."
دارل مجدداً گفت: "مشتریان می توانند به دلایل زیادی از ما شکایت کنند که البته نمی خواهم آنها را در اینجا بیان کنم. سرقت های دیگر می توانند حتی باعث شکایت مشتریان، بانک ها و سرمایه گذاران از ما شوند. ما چه برنده شویم و چه بازنده، باید هزینه های این موضوع را خودمان بپردازیم. اتفاقاً این موضوعی است که سر و صدای زیادی در رسانه ها به پا خواهد کرد."
آدریتو در پاسخ گفت: "حداقل، آیا نیاز است که این قدر سریع، موضوع را به اطلاع مشتریانمان برسانیم؟"
دارل در پاسخ گفت: "در سه ایالت که شرکت در آنها فعال است، اعلام سریع اجباری است اما در سه ایالت دیگر این چنین نیست. اما تا آنجا که من فهمیده ام، شما نمی دانید احتمالاً فلایتون چه نقشی در ارتکاب این جرم داشته است. بانک اشکالی را شناسایی کرده است. به نظر می رسد میان کارت های جعلی و کارت هایی که از آنها برای خرید از فروشگاه های فلایتون استفاده شده است، رابطه ای مستقیم وجود دارد. البته ممکن است این موضوع، اتفاقی هم باشد. متأسفانه ما هنوز منشأ این سوءاستفاده را نمی دانیم."
برت پرسید: "حالا باید چه کار کنیم. ما به دنبال این نیستیم که کاری نکنیم و دست روی دست بگذاریم. حداقل برای من که چنین است."
دارل در حالی که آدریتو را خطاب قرار داده بود، با تأکید گفت: "این دقیقاً کاری است که باید انجام دهید. استراتژی ارتباطی شما نباید حرف نزدن با دیگران باشد. اگر از رسانه‌ها با شما تماس گرفته شد، موضوع را تأیید کنید و بگویید که فلایتون موضوع را به اطلاع مقامات انتظامی رسانده است و ما اکنون منتظر تکمیل تحقیقات آنها و دستیابی به اطلاعات نهایی هستیم. آنها را به سازمان اطلاعات و امنیت ارجاع دهید. آنها هیچ چیزی به دیگران نخواهند گفت."
برت گفت: "این روش برای شرایط فعلی کارآمد است اما سالی از شما می خواهم گام های بعدی را هم پیش بینی کنید. من می خواهم اطلاعات درست ارایه کنیم نه موضوعاتی مبهم و در لفافه."

برت می دانست که هیچ پاسخ ساده ای را نمی توان برای این مشکل پیچیده یافت. تحقیق الکترونیکی شب گذشتهٔ او، نشان می داد مشتریان علاقه مند نیستند از فروشگاه هایی خرید کنند که احتمال سرقت اطلاعات در آنها وجود دارد. دارل معتقد بود که اگر فلایتون سریعاً اخبار را منتشر کند، میزان آسیب پذیری خود را افزایش داده است. اما آیندهٔ شرکت به شهرت آن در رعایت عدالت و شفافیت در کارهایش بستگی داشت - اینها میراث پدر برت پس از سال ها تلاش و کوشش بودند.
سالی گفت: "بسیار خوب اما این راه حلی موقتی است. من حساب های آلوده شده را بررسی کردم و به یک نام جالب رسیدم یعنی دیو استیونس[13] که سردبیر بخش شبانگاهی اخبار کانال TV-KCDK است. ظاهراً ما یک تلویزیون سینمای خانگی برای او نصب کرده ایم. چنین مواردی همیشه خطرات خاص خود را دارند."
برت جایش را عوض کرد، از جای خود برخاست و گفت: "اگر درست فهمیده باشم، ما دلیلی مشروط اما قوی داریم که سرقتی رخ داده، دو کارمند داریم که ممکن است در این کار دخالت داشته باشند یا نداشته باشند، برخی ایالت ها ما را ملزم می سازند که چنین اطلاعاتی را در اختیار مردم قرار دهیم و دیگر ایالت ها چنین الزامی برای ما ندارند. اگر ما موضوع را افشا کنیم، از ما شکایت می شود و اگر افشا نکنیم، باعث بی اعتمادی مشتریانمان خواهیم شد."
در نهایت، برت باید تصمیم آخر را میگرفت. او به تک تک اعضای تیم مدیریتی خود نگاه کرد. چشمان او برقی از امید زدند. او اعتماد کامل به این افراد داشت. لذا با کلماتی شمرده و آرام، خطاب به آنها گفت: "از یک موضوع مطمئن هستم. نام فلایتون، برای من، برای کارکنانم و برای مشتریان نامی همراه با اعتبار و اعتماد است. بنابراین هر تصمیمی که امروز تیم بگیرد، به اجرا گذارده خواهد شد تا این اعتبار و اعتماد حفظ شود.
شرکت فلایتون الکترونیک باید چگونه به این وضعیت پاسخ دهد؟ در ادامه پاسخ های چهار متخصص را می خوانید.

اینکه شما چگونه نسبت به یک مشکل امنیتی واکنش نشان دهید از خود آنچه که رخ داده، مهمتر است. همچنین اینکه کسب و کار شما بتواند از این مهلکه جان سالم به در ببرد، به تصمیم درستی بستگی دارد که شما باید اتخاذ کنید و آن را به اطلاع سهامداران متعدد خود برسانید. تجربهٔ شرکت من، یک نمونهٔ جالب است.

13.Dave Stevens

جیمز لی[14] قایم مقام و مدیر بخش روابط عمومی و امور مشتریان شرکت چویسپوینت[15] در آلفارتا[16]، ایالت جرجیا[17]

اینکه شما چگونه نسبت به یک مشکل امنیتی واکنش نشان دهید از خود آنچه که رخ داده، مهم تر است. همچنین اینکه کسب و کار شما بتواند از این مهلکه جان سالم به در ببرد، به تصمیم درستی بستگی دارد که شما باید اتخاذ کنید و آن را به اطلاع سهامداران متعدد خود برسانید. تجربهٔ شرکت من، یک نمونهٔ جالب است.

چویس پوینت در زمینهٔ کمک و مشاوره دادن به تصمیم گیری شرکت ها و دولت ها فعال است و این کار را از طریق شناسایی، گردآوری، تجزیه و تحلیل و ارایهٔ اطلاعات مربوط به افراد و سازمان ها انجام می دهد. در سال ۲۰۰۵، شرکت ما قربانی یک کلاهبرداری شد که در جریان آن مجرمان به عنوان مشتری وارد سایت ما شدند و اطلاعات ۱۴۵۰۰۰ مشتری ما را دزدیدند. هیچ گونه سوءاستفاده ای از فن آوری موجود رخ نداده بود اما رسانه ها طوری برخورد کردند که گویی این چنین بوده است. ما فعالیت های شیطانی این مجرمان را به ادارهٔ پلیس لس آنجلس گزارش کردیم. به کمک آنها و در جریان عملیاتی یک باند جنایی نیجریه ای متلاشی شد.

ما توانسته بودیم یک استراتژی درست را به کار گیریم و نهایتا به این نتیجه رسیدیم که به مشتریانی که ممکن بود از اطلاعاتشان سوءاستفاده شده باشد، بدون توجه به محل سکونتشان خبر دهیم. ما کارکنان‌مان را توجیه کردیم و چند نشست را با حضور مدیران و افسران پلیس برگزار کردیم. مدیر عامل و دیگر مدیران ارشد ما با مشتریان و سرمایه گذاران کلیدی ملاقات کردند تا سیاست ها و روندهای جدیدی را که برای جلوگیری از رخ دادن مجدد چنین اتفاقی اتخاذ کرده بودیم به اطلاع آنها برسانند. آنها کسانی بودند که نقش بسزایی در حیات دوبارهٔ ما داشتند.

برخی از اقدامات پیشگیرانهٔ ما بسیار اساسی بودند. مثلاً ما یکی از بخش های کسب و کارمان را که ارزشی ۲۰ میلیون دلاری داشت، متوقف کردیم زیرا احتمال نقض اطلاعات آن بسیار بالا بود. تغییرات فرهنگی در کارکنان نیز لازم بود. لذا اکنون کارمندان ما موظف هستند تا به عنوان شرط ادامهٔ کارشان، دوره های آموزشی و امنیتی را بگذرانند.

در شرکت چویس پوینت، ما به سرعت دریافتیم که در چنین مواقعی، عوامل بسیاری وجود دارند که خارج از کنترل ما هستند. رسانه ها می توانند نقش مخربی ایفا کنند. البته شرایط از این هم وخیم تر است. شما ناگهان با حجم انبوهی از تقاضای روزنامه ها، مجلات و سایر رسانه ها مواجه می‌شوید.

حتی شما باید به دادستان ایالتی، نمایندهٔ کمیسیون تجارت فدرال و حتی نمایندهٔ کنگرهٔ آمریکا پاسخگو باشید. ممکن است بانک ها از شما به دادگاه شکایت کنند. افرادی که کارت های اعتباری شما را دارند و شرکت هایی که مسئول پردازش اطلاعات کارت های صادر شده بوسیله شما هستند و مصرف کنندگان نیز ممکن است از شما شکایت کنند. حتی شما با شکایاتی از جانب کارکنان و بازنشستگان شرکت خود مواجه می شوید.

برای فلایتون الکترونیک نیز چنین شرایطی در مواجهه با این بحران وجود دارد. زمان بندی، یک عنصر حیاتی در شکایت ها است. این امر باعث می شود که مدیران شرکت در صورت مواجهه با چنین شکایاتی تمرکزشان را از دست ندهند. برای رفع نقاط ضعف شرکت در قبال امنیت اطلاعات، برت فلایتون مدیر این شرکت باید استراتژی احیای نام تجاری شرکتش را تدوین کند این شرکت باید همانند چویس پوینت، سریعا تمامی مشتریان در معرض خطر خود را مطلع کند، تلفن هایی رایگان را برای ارایهٔ اطلاعات به مشتریان دایر کند و از خدمات نظارت بر کارت های اعتباری بهره ببرد. آنها باید با تلاش زیاد وفاداری مشتریانشان را حفظ کنند. آنها می توانند به کمک تخفیف یا فروش با شرایط مناسب، تا حدی از حجم انتقادها بکاهند. همچنین آنها باید در سیاست ها و رویه های خود تجدیدنظر کنند.

در نهایت، فلایتون و همکارانش نباید صبر و شکیبایی خود را از دست بدهند. تا زمانی که توجه به این مشکل در اذهان عمومی و رسانه ها وجود دارد، این مسئله حل نخواهد شد. باید اثرات این معضل بر نام تجاری و شهرت و اعتبار شرکت را تقلیل داد. من پیش بینی می کنم که فلایتون الکترونیک برای رها شدن از این وضعیت به سه تا پنج سال زمان نیاز دارد.

بیل بونی[18]، مدیر امنیت اطلاعات شرکت موتورولا[19] در شامبرگ[20]، ایلینویز[21]. او همچنین نایب رییس و عضو هیأت مدیرهٔ انجمن کنترل و ممیزی سیستم های اطلاعاتی[22] است که یک سازمان جهانی مستقر در رولینگ میدوز[23]، ایلی نویز است.

اکثر مدیران ارشد دارای معیارها و ابزارهایی برای ارزیابی خسارات ناشی از بلایای ملموس همانند سیل و آتش سوزی هستند. اما این امر در مورد امنیت اطلاعات به ویژه پیشگیری و برنامه ریزی در مورد سرقت اطلاعات مصداق ندارد. شرکت‌هایی که توجه خاصی به مصون نگاه داشتن اطلاعات و حفظ ارزش آنها دارند، از یک مدیر یا نایب رییس مصونیت

14.James Lee
15.Choice Point
16.Alpharetta
17.Georgia

18.Bill Boni
19.Motorola
20.Schaumberg
21.Illinois
22.Information Systems Audit and Control Association
23.Rolling Meadows

اطلاعات استفاده می کنند که نه تنها مدیر است بلکه برترین فرد در این عرصه است.

هفت سال پیش، من به عنوان نخستین مدیر مصونیت اطلاعات شرکت موتورولا منصوب شدم. به عنوان یک رهبر مسئول مصونیت اطلاعات، من مسئول اطلاعات و محیط جهانی فن آوری اطلاعات شرکت هستم و از یک استراتژی جامع در قبال مدیریت ریسک بهره می برم. یکی از عناصر مفید این استراتژی، شناسایی روش های جدید در مورد اطلاعات و حفظ ارزش آنها است. این امر می تواند باعث ایجاد موانع امنیتی مناسبی برای طرح های اطلاعاتی شود. این امر همچنین برای سیاست ها، روندها و پروتکل های آموزشی نیز مفید است.

البته باید توجه داشت که فن آوری ها هر روزه در حال ارتقا یافتن هستند و این امر کار مصونیت و حفظ اطلاعات را دشوار می سازد. حتی یک مرتبه هک کردن اطلاعات یک شرکت می‌تواند به یک بحران واقعی تبدیل شود. من سازمان هایی را

البته باید توجه داشت که فن آوری ها هر روزه در حال ارتقا یافتن هستند و این امر کار مصونیت و حفظ اطلاعات را دشوار می سازد. حتی یک مرتبه هک کردن اطلاعات یک شرکت می‌تواند به یک بحران واقعی تبدیل شود. من سازمان هایی را

دیده ام که میلیون ها دلار صرف موانع امنیتی می کنند اما افراد دارای دانش کافی می توانند به راحتی از این حفاظ های امنیتی بگذرند. مثلاً موتورولا به یکی از مشتریانش که رقم هنگفتی صرف ایجاد بهترین حفاظ های اطلاعاتی موجود کرده بود، ثابت کرد که می توان از طریق اینترنت به محوری ترین سیستم‌های اطلاعاتی آن دست یافت.

برای پیشگیری و مقابله با نقض اطلاعات، شما باید افرادی را در اختیار داشته باشید که از تخصص کافی در این زمینه برخوردارند و می توانند سیستم ها را به خوبی درک کنند. مصونیت اطلاعات الزاماً یک صلاحیت محوری در مورد فن‌آوری اطلاعات یا در مورد یک تیم نیست که هدفش جلوگیری از خسارات است. همچنین آنها باید آشنایی خوبی با قوانین و استانداردهای موجود داشته باشند.

با توجه به حقایق بیان شده، فلایتون باید در وهلهٔ اول مراجع انتظامی را مطلع سازد تا هم مشتریان و هم اعتبارش را حفظ کند. فلایتون نمی تواند مدت زمانی طولانی این موضوع را از عموم مخفی نگاه دارد. البته این شرکت باید نهایت همکاری را با سازمان اطلاعات و امنیت داشته باشد اما اولویت آن باید حفظ اعتماد مردم و در عین حال رعایت کامل قوانین مصونیت اطلاعات و حفظ حریم خصوصی افراد در ایالت هایی باشد که اطلاعاتشان به سرقت رفته اند.

جان فیلیپ کوگلان[24] رییس و مدیر عامل سابق شرکت ویزا آمریکا[25] است که مقر آن در سانفرانسیسکو[26] است نقض اطلاعات می تواند یک مدیر را در یک وضعیت به شدت پیچیده قرار دهد و این در شرایطی است که او با انبوهی از سهامداران صحبت کرده و شرایط را برای آنها توضیح دهد. این موضوعی است که مدیر عامل شرکت فلایتون الکترونیک نیز با آن مواجه شده است.

بانک هایی همچون یونیون سنچری که این کارتها را صادر کرده اند، اولین کسانی هستند که متوجه این موضوع می شوند به ویژه زمانی که سیستم هایشان چنین مواردی را تشخیص می دهند. برای مصونیت دارندگان کارت های اعتباری، باید این روند شناسایی در همان مراحل نخست کلاهبرداری صورت بپذیرد.

بانک ها باید حساسیت بالاتری در این زمینه از خود نشان دهند. البته بانک یونیون سنچری مسئول پرداخت کارت های ویزا کارت و مستر کارت است که جزء بهترین استانداردهای این صنعت هستند. بنابراین، نام تجاری، منافع و اعتبار بانک صادرکننده نیز به خطر افتاده است.

آنچه که این موضوع را پیچیده تر می سازد، نقش نیروهای انتظامی است. سازمان اطلاعات و امنیت از فلایتون خواسته است تا این موضوع را فاش نکند زیرا اعتقاد دارد که آسیب پذیری این سیستم در زمان نظارت و تحقیق توسط این سازمان، بهترین شرایط را برای سارقان فراهم می آورد تا فعالیت های خود را از سر بگیرند. متأسفانه چنین درخواست هایی فقط اوضاع را بدتر می کنند و امکان سوء استفاده از شرکت بیشتر می شود. رد این گونه درخواست های مراجع انتظامی

24.John Philip Coghlan
25.Visa America
26.San Francisco

غیرقانونی نیست. بر عکس، بسیاری از قوانین ایالتی این گونه شرکت ها را ملزم می سازند تا اطلاعات را به موقع فاش کنند. علاوه بر سهامداران، گروه هایی همچون مصرف کنندگان، قانونگذاران و کارکنان نیز وجود دارند که باید منافعشان را به دقت مد نظر قرار داد. در مورد مشتریان، احتمالاً مدیر عامل از تحقیقات صورت گرفته دریافته است که ۷۸ درصد افراد اعلام کرده اند دیگر از فروشگاه های این شرکت خرید نخواهند کرد. این خبر بدی برای برت فلایتون است.

بنابراین مدیر عامل فلایتون هیچ چاره ای جز فاش کردن اطلاعات ندارد. اگر او حرفی نزند، در واقع مشتریان را از بهترین ابزار محافظت کننده از خود محروم کرده است. آنها با استمرار استفاده از کارت هایشان تنها کار سارقان را راحت‌تر می کنند. حتی اگر او بخواهد منتظر باشد تا به اطلاعات بیشتری دست یابد، باید علیرغم نداشتن اطلاعات کامل، موضوع را نزد افکار عمومی مطرح کند. در عین حال اگر او این موضوع را اعلام نکند، ممکن است دیگران این کار را انجام دهند و در نتیجه او باید به دفاع از خود هم بپردازد. این شرکت شهرت خود را مدیون صداقتش است و بنابراین برت و مشاورانش نباید هرگز این موضوع را فراموش کنند.

جی فولی[۲۷] مدیر اجرایی بخش مرکز منابع شناسایی سرقت در ساندیگو[۲۸]

مدیران شرکت فلایتون الکترونیک به دلیل گفته های دارل هانتینگتون که مشاوری از خارج سازمانشان است، دچار اشتباه شده اند. شرکت هایی که از آنها در دادگاه شکایت می شود و تحت پیگرد قضایی قرار می گیرند، آنانی نیستند که به عنوان اولین نفر موضوع نقض اطلاعات را نزد عموم مطرح می کنند بلکه آنانی هستند که به شکلی ضعیف عمل می کنند. فلایتون هیچ شانسی ندارد جز اطلاع رسانی مناسب. اعلام اطلاعات غلط و سپس اصلاح آنها، به اندازهٔ خود نقض و سرقت اطلاعات مشکل ساز است. اکنون فلایتون باید آرامش خود را حفظ کند اما نه به آن دلایلی که دارل هانتینگتون گفته بود. دیگر سوء تفاهم و در واقع سوء برداشت تیم مدیریت شرکت فلایتون آن است که آنها باید خودشان موضوع را به اطلاع مشتریانشان برسانند. معاملات مربوط به کارت های اعتباری متعلق به یک بانک هستند که می تواند تعداد دارندگان کارت‌هایش را برآورد کند. فلایتون نباید خود را درگیر یافتن آدرس مشتریان و اطلاع رسانی به آنها کند زیرا این امر می‌تواند مشکلات حقوقی به دنبال داشته باشد. مثلاً ممکن است دارندگان این کارت ها نخواهند که کسی جز بانک به آدرس آنها دسترسی داشته باشد و با آنها تماس بگیرد. کسان دیگری در این زنجیره همچون شرکت پردازش کنندهٔ اطلاعات معاملات نیز به اندازهٔ دیگران مقصر است. در حقیقت، این امکان وجود دارد که تحقیقات سازمان اطلاعات و امنیت نشان دهند که شرکت فلایتون الکترونیک ارایه کنندهٔ خدمات الکترونیکی اصلاً مقصر نبوده است.

مراجع انتظامی از مسئولان این شرکت خواسته اند سکوت اختیار کنند تا آنها کارشان را انجام دهند و فرصت بهتری برای تعقیب و دستگیری مجرمان داشته باشند. از سوی دیگر، اگر فلایتون موضوع را علنی کند، مجرمان فرصت خواهند داشت تا ناپدید شوند و بدین ترتیب هیچ نتیجه ای عاید نخواهد شد. به نظر من برت فلایتون به عنوان مدیر عامل شرکت باید با آرامش کامل دربارهٔ بحران پیش آمده بیاندیشد. عدم اطلاع رسانی به مشتریان بدان معنا نیست که او باید یک جا بنشیند، دست روی دست بگذارد و کاری انجام ندهد. اولین کار شرکت باید نظارت دقیق بر حساب ها و پر کردن هر روزنه ای باشد که احتمال ورود از آن به حساب های مشتریان وجود دارد. البته این کار باید به طریقی انجام شود که خللی در فعالیت‌های سازمان اطلاعات و امنیت ایجاد نکند. مدیران شرکت باید رویه ها و سیاست های خود را مورد ارزیابی مجدد قرار دهند و باید قوانین را برای ارزیابی برنامه ریزی استراتژیک و خود ممیزی به اجرا درآورند. سرگئی که مدیر بخش اطلاعات است، هیچ شانسی برای خطا کردن ندارد.

شاید نگران کننده ترین موضوع که به مراتب فراتر از مشکل پیش آمده برای فلایتون الکترونیک است، این است که فعالیت‌های مجرمانه در صنعت اطلاعات به شدت در حال رشد است. امروزه می توان با صرف پولی اندک به انبوهی اطلاعات دربارهٔ نام افراد، شمارهٔ تأمین اجتماعی آنها و حتی تاریخ تولدشان دست یافت. اگر مجرمان فهرستی بلند از این اطلاعات داشته باشند، می توانند به ثروت برسند. این واقعیتی است که نمایانگر نیاز به افزایش تلاش های ما برای حفظ و مصونیت هر چه بیشتر داده های فردی است. ما باید حفظ و مصونیت اطلاعات را واقعاً جدی بگیریم.

27.Jay Foley
28.San Diego