START WITH SECURITY

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

FEDERAL TRADE COMMISSION

START WITH SECURITY

1. **Start with security.**
2. **Control access to data sensibly.**
3. **Require secure passwords and authentication.**
4. **Store sensitive personal information securely and protect it during transmission.**
5. **Segment your network and monitor who's trying to get in and out.**
6. **Secure remote access to your network.**
7. **Apply sound security practices when developing new products.**
8. **Make sure your service providers implement reasonable security measures.**
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**
10. **Secure paper, physical media, and devices.**

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlined in *Protecting Personal Information: A Guide for Business,* you should know what personal information you have in your files and on your computers, and keep only what you need for your business. You should protect the information that you keep, and properly dispose of what you no longer need. And, of course, you should create a plan to respond to security incidents.

In addition to *Protecting Personal Information*, the FTC has resources to help you think through how those principles apply to your business. There's an online tutorial to help train your employees; publications to address particular data security challenges; and news releases, blog posts, and guidance to help you identify – and possibly prevent – pitfalls.

There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1 Start with security.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. Experts agree on the key first step: Start with security. Factor it into the decisionmaking in every department of your business – personnel, sales, accounting, information technology, etc. Collecting and maintaining information "just because" is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business. Lessons from FTC cases illustrate the benefits of building security in from the start by going lean and mean in your data collection, retention, and use policies.

Don't collect personal information you don't need.

Here's a foundational principle to inform your initial decision-making: No one can steal what you don't have. When does your company ask people for sensitive information? Perhaps when they're registering online or setting up a new account. When was the last time you looked at that process to make sure you really need everything you ask for? That's the lesson to learn from a number of FTC cases. For example, the FTC's complaint against ***RockYou*** charged that the company collected lots of information during the site registration process, including the user's email address and email password. By collecting email passwords – not something the business needed – and then storing them in clear text, the FTC said the company created an unnecessary risk to people's email accounts. The business could have avoided that risk simply by not collecting sensitive information in the first place.

Hold on to information only as long as you have a legitimate business need.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the FTC's ***BJ's Wholesale Club*** case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

Don't use personal information when it's not necessary.

You wouldn't juggle with a Ming vase. Nor should businesses use personal information in contexts that create unnecessary risks. In the ***Accretive*** case, the FTC alleged that the company used real people's personal information in employee training sessions, and then failed to remove the information from employees' computers after the sessions were over. Similarly, in ***foru International***, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.

2 Control access to data sensibly.

Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. You'll want to keep it from the prying eyes of outsiders, of course, but what about your own employees? Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need to know" basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. When thinking about how to control access to sensitive information in your possession, consider these lessons from FTC cases.

Restrict access to sensitive data.

If employees don't have to use personal information as part of their job, there's no need for them to have access to it. For example, in ***Goal Financial***, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people's personal information.

Limit administrative access.

Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job. In its action against ***Twitter***, for example, the FTC alleged that the company granted almost all of its employees administrative control over Twitter's system, including the ability to reset user account passwords, view users' nonpublic tweets, and send tweets on users' behalf. According to the complaint, by providing administrative access to just about everybody in-house, Twitter increased the risk that a compromise of any of its employees' credentials could result in a serious breach. How could the company have reduced that risk? By ensuring that employees' access to the system's administrative controls was tailored to their job needs.

3 Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password "hygiene" – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are tips to take from FTC cases.

Insist on complex and unique passwords.

"Passwords" like 121212 or qwerty aren't much better than no passwords at all. That's why it's wise to give some thought to the password standards you implement. In the ***Twitter*** case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

Store passwords securely.

Don't make it easy for interlopers to access passwords. In ***Guidance Software***, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in ***Reed Elsevier***, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In ***Twitter***, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely. Businesses also may want to consider other protections – two-factor authentication, for example – that can help protect against password compromises.

Guard against brute force attacks.

Remember that adage about an infinite number of monkeys at an infinite number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password. In the ***Lookout Services***, ***Twitter***, and ***Reed Elsevier*** cases, the FTC alleged that the businesses didn't suspend or disable user credentials after a certain number of unsuccessful login attempts. By not adequately restricting the number of tries, the companies placed their networks at risk. Implementing a policy to suspend or disable accounts after repeated login attempts would have helped to eliminate that risk.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is left open. In ***Lookout Services***, the FTC charged that the company failed to adequately test its web application for widely-known security flaws, including one called "predictable resource location." As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

4 Store sensitive personal information securely and protect it during transmission.

For many companies, storing sensitive data is a business necessity. And even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. But regardless of the method, it's only as good as the personnel who implement it. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. With that in mind, here are a few lessons from FTC cases to consider when securing sensitive information during storage and transmission.

Keep sensitive information secure throughout its lifecycle.

Data doesn't stay in one place. That's why it's important to consider security at all stages, if transmitting information is a necessity for your business. In ***Superior Mortgage Corporation***, for example, the FTC alleged that the company used SSL encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, and not just during the initial transmission.

Use industry-tested and accepted methods.

When considering what technical standards to follow, keep in mind that experts already may have developed effective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary. Instead, they take advantage of that collected wisdom. The ***ValueClick*** case illustrates that principle. According to the FTC, the company stored sensitive customer information collected through its e-commerce sites in a database that used a non-standard, proprietary form of encryption. Unlike widely-accepted encryption algorithms that are extensively tested, the complaint charged that ValueClick's method used a simple alphabetic substitution system subject to significant vulnerabilities. The company could have avoided those weaknesses by using tried-and-true industry-tested and accepted methods for securing data.

Ensure proper configuration.

Encryption – even strong methods – won't protect your users if you don't configure it properly. That's one message businesses can take from the FTC's actions against ***Fandango*** and ***Credit Karma***. In those cases, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

5 Segment your network and monitor who's trying to get in and out.

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Segment your network.

Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network. That's a lesson from the ***DSW*** case. The FTC alleged that the company didn't sufficiently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks. The company could have reduced that risk by sufficiently segmenting its network.

Monitor activity on your network.

"Who's that knocking on my door?" That's what an effective intrusion detection tool asks when it detects unauthorized activity on your network. In the ***Dave & Buster's*** case, the FTC alleged that the company didn't use an intrusion detection system and didn't monitor system logs for suspicious activity. The FTC says something similar happened in ***Cardsystem Solutions***. The business didn't use sufficient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company's network that collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks.

6 Secure remote access to your network.

Business doesn't just happen in the office. While a mobile workforce can increase productivity, it also can pose new security challenges. If you give employees, clients, or service providers remote access to your network, have you taken steps to secure those access points? FTC cases suggest some factors to consider when developing your remote access policies.

Ensure endpoint security.

Just as a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it. That's the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For example, in ***Premier Capital Lending***, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business's security. When hackers accessed the client's system, they stole its remote login credentials and used them to grab consumers' personal information. According to the complaint in ***Settlement One***, the business allowed clients that didn't have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal. And in ***Lifelock***, the FTC charged that the company failed to install antivirus programs on the computers that employees used to remotely access its network. These businesses could have reduced those risks by securing computers that had remote access to their networks.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. That's why it's wise to limit access to what's needed to get the job done. In the ***Dave & Buster's*** case, for example, the FTC charged that the company failed to adequately restrict third-party access to its network. By exploiting security weaknesses in the third-party company's system, an intruder allegedly connected to the network numerous times and intercepted personal information. What could the company have done to reduce that risk? It could have placed limits on third-party access to its network – for example, by restricting connections to specified IP addresses or granting temporary, limited access.

7 Apply sound security practices when developing new products.

So you have a great new app or innovative software on the drawing board. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely? Before going to market, consider the lessons from FTC cases involving product development, design, testing, and roll-out.

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? In cases like ***MTS***, ***HTC America***, and ***TRENDnet***, the FTC alleged that the companies failed to train their employees in secure coding practices. The upshot: questionable design decisions, including the introduction of vulnerabilities into the software. For example, according to the complaint in ***HTC America***, the company failed to implement readily available secure communications mechanisms in the logging applications it pre-installed on its mobile devices. As a result, malicious third-party apps could communicate with the logging applications, placing consumers' text messages, location data, and other sensitive information at risk. The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.

Follow platform guidelines for security.

When it comes to security, there may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts. In actions against ***HTC America***, ***Fandango***, and ***Credit Karma***, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned off a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for developers, which explicitly warn against turning off SSL certificate validation.

Verify that privacy and security features work.

If your software offers a privacy or security feature, verify that the feature works as advertised. In ***TRENDnet***, for example, the FTC charged that the company failed to test that an option to make a consumer's camera feed private would, in fact, restrict access to that feed. As a result, hundreds of "private" camera feeds were publicly available. Similarly, in ***Snapchat***, the company advertised that messages would "disappear forever," but the FTC says it failed to ensure the accuracy of that claim. Among other things, the app saved video files to a location outside of the app's sandbox, making it easy to recover the video files with common file browsing tools. The lesson for other companies: When offering privacy and security features, ensure that your product lives up to your advertising claims.

Test for common vulnerabilities.

There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in the ***Guess?*** case, the FTC alleged that the business failed to assess whether its web application was vulnerable to Structured Query Language (SQL) injection attacks. As a result, hackers were able to use SQL attacks to gain access to databases with consumers' credit card information. That's a risk that could have been avoided by testing for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).

8 Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In ***GMR Transcription***, for example, the FTC alleged that the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed on the internet. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can't be a "take our word for it" thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process. The ***Upromise*** case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to "remove any personally identifiable information" before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted it in clear text. How could the company have reduced that risk? By asking questions and following up with the service provider during the development process.

9 Put procedures in place to keep your security current and address vulnerabilities that may arise.

Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up. If you use third-party software on your networks, or you include third-party software libraries in your applications, apply updates as they're issued. If you develop your own software, how will people let you know if they spot a vulnerability, and how will you make things right? FTC cases offer points to consider in thinking through vulnerability management.

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. In the ***TJX Companies*** case, for example, the FTC alleged that the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Depending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.

Heed credible security warnings and move quickly to fix them.

When vulnerabilities come to your attention, listen carefully and then get a move on. In the ***HTC America*** case, the FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions. Sometimes, companies receive security alerts, but they get lost in the shuffle. In ***Fandango***, for example, the company relied on its general customer service system to respond to warnings about security risks. According to the complaint, when a researcher contacted the business about a vulnerability, the system incorrectly categorized the report as a password reset request, sent an automated response, and marked the message as "resolved" without flagging it for further review. As a result, Fandango didn't learn about the vulnerability until FTC staff contacted the company. The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security@yourcompany.com) for receiving reports and flagging them for your security staff.

10 Secure paper, physical media, and devices.

Network security is a critical consideration, but many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives, and disks. FTC cases offer some things to consider when evaluating physical security at your business.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. In the ***Gregory Navone*** case, the FTC alleged that the defendant maintained sensitive consumer information, collected by his former businesses, in boxes in his garage. In ***Lifelock***, the complaint charged that the company left faxed documents that included consumers' personal information in an open and easily accessible area. In each case, the business could have reduced the risk to their customers by implementing policies to store documents securely.

Protect devices that process personal information.

Securing information stored on your network won't protect your customers if the data has already been stolen through the device that collects it. In the 2007 ***Dollar Tree*** investigation, FTC staff said that the business's PIN entry devices were vulnerable to tampering and theft. As a result, unauthorized persons could capture consumer's payment card data, including the magnetic stripe data and PIN, through an attack known as "PED skimming." Given the novelty of this type of attack at the time, and a number of other factors, staff closed the investigation. However, attacks targeting point-of-sale devices are now common and well-known, and businesses should take reasonable steps to protect such devices from compromise.

Keep safety standards in place when data is en route.

Savvy businesses understand the importance of securing sensitive information when it's outside the office. In ***Accretive***, for example, the FTC alleged that an employee left a laptop containing more than 600 files, with 20 million pieces of information related to 23,000 patients, in the locked passenger compartment of a car, which was then stolen. The ***CBR Systems*** case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive – all of which contained sensitive information – that were lifted from an employee's car. In each case, the business could have reduced the risk to consumers' personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets you track where the package is. Limit the instances when employees need to be out and about with sensitive data in their possession. But when there's a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.

Dispose of sensitive data securely.

Paperwork or equipment you no longer need may look like trash, but it's treasure to identity thieves if it includes personal information about consumers or employees. For example, according to the FTC complaints in ***Rite Aid*** and ***CVS Caremark***, the companies tossed sensitive personal information – like prescriptions – in dumpsters. In ***Goal Financial***, the FTC alleged that an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The companies could have prevented the risk to consumers' personal information by shredding, burning, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

Looking for more information?

The FTC's Business Center (**business.ftc.gov**) has a Data Security section with an up-to-date listing of relevant cases and other free resources.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at **business.ftc.gov**.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman.**

Federal Trade Commission
business.ftc.gov
June 2015

COMIENCE CON SEGURIDAD

UNA GUÍA PARA NEGOCIOS

LECCIONES APRENDIDAS DE LOS CASOS DE LA FTC.

LA COMISIÓN FEDERAL DE COMERCIO

COMIENCE CON SEGURIDAD

1. Comience con la seguridad.
2. Controle prudentemente el acceso a los datos.
3. Exija el uso de contraseñas seguras y un procedimiento de autentificación.
4. Archive la información personal delicada de manera segura y protéjala durante la transmisión.
5. Segmente su red y haga un monitoreo para controlar quién está tratando de entrar y salir.
6. Proteja el acceso remoto a su red informática.
7. Aplique prácticas de seguridad sólidas al desarrollo de nuevos productos.
8. Controle que sus proveedores de servicio implementen medidas de seguridad lógicas.
9. Implemente procedimientos para mantener actualizada su seguridad y ocúpese de solucionar las vulnerabilidades que pudieran surgir.
10. Guarde en un lugar seguro los archivos de papel y los medios y dispositivos de almacenamiento.

Cuando usted maneja su red informática, desarrolla una aplicación o incluso cuando organiza sus archivos impresos en papel, la implementación de una seguridad sólida en su negocio no es algo fortuito. Las compañías que consideran la seguridad desde el comienzo pueden evaluar sus opciones y tomar decisiones basadas en la naturaleza de su negocio y en el nivel de vulnerabilidad de la información que manejan. Las amenazas contra los datos pueden transformarse con el transcurso del tiempo, pero los fundamentos de una seguridad sólida permanecen constantes. Tal como lo señaló la FTC en su publicación *Cómo proteger la información personal: una guía para negocios,* usted debe saber cuál es la información que archiva en sus registros y en sus computadoras, y conservar únicamente aquella información que necesite para operar su negocio. Usted debe proteger la información que mantiene en archivo y eliminar debidamente los datos que no necesite. Y por supuesto, debe crear un plan para responder a los incidentes de seguridad.

Además de la guía *Cómo proteger la información personal,* la FTC tiene otros recursos para ayudarlo a analizar cómo puede aplicar esos principios en su negocio. Hay un tutorial en línea que le será útil para capacitar a sus empleados; publicaciones para abordar desafíos particulares de la seguridad de datos; y noticias, artículos de blog, y orientación para ayudarlo a identificar – y posiblemente prevenir – inconvenientes.

También existe otra fuente de información sobre la protección de datos delicados: las lecciones aprendidas a partir de las más de 50 acciones de cumplimiento de ley anunciadas por la FTC hasta la fecha. Obviamente, estos acuerdos resolutorios – la corte no adoptó ninguna una resolución sobre los casos – y los detalles específicos de las órdenes se aplican exclusivamente a esas compañías. Pero las lecciones aprendidas a partir de los errores que originaron las acciones de cumplimiento de ley pueden ayudarlo a mejorar las prácticas de su compañía. Y la mayoría de las prácticas alegadas en esos casos involucra errores de seguridad básicos y fundamentales. Mediante un exhaustivo análisis de los hechos de esos casos, le ofrecemos diez lecciones para aprender en detalle cuáles son las vulnerabilidades que podrían afectar a su compañía, junto con orientación práctica sobre cómo reducir los riesgos que plantean.

1 Comience con la seguridad.

Los datos delicados, desde la información personal de las solicitudes de empleo hasta los archivos de las redes informáticas que contienen los números de tarjeta de crédito de los clientes, están omnipresentes en muchas compañías. Los ejecutivos de los negocios suelen preguntar cómo se debe manejar la información confidencial. Los expertos concuerdan en el primer paso clave: comience con seguridad. Incluya el factor seguridad en el proceso de toma de decisiones de cada sección de su negocio – personal, ventas, contabilidad, tecnología de la información, etc. Recolectar información y guardarla "solo porque sí" ya no es una estrategia comercial sólida. Las compañías inteligentes piensan detenidamente las implicaciones de las decisiones sobre la seguridad de sus datos. Usted puede reducir el riesgo de que surjan incidentes de datos en el futuro tomando decisiones meditadas acerca del tipo de información que recolecta su negocio, cuánto tiempo la conserva y quiénes pueden acceder a los datos. Por supuesto que todas esas decisiones dependerán de la naturaleza de su negocio. Las lecciones que surgen de los casos de la FTC ilustran los beneficios de construir la seguridad desde el inicio preparando y perfeccionando sus políticas de recolección, retención y uso de datos.

No recolecte información personal que no necesite.

Este es un principio fundacional que debe considerar en sus decisiones iniciales: nadie puede robarle lo que no tiene. ¿Cuándo le solicita información delicada a la gente? Quizás cuando se registra en internet o establece una cuenta nueva con su compañía. ¿Cuándo fue la última vez que revisó ese proceso para determinar que realmente necesita todos los datos que está solicitando su negocio? Esa es una de las lecciones que se puede aprender a partir de una cantidad de casos de la FTC. Por ejemplo, en la demanda de la FTC contra ***RockYou*** se acusó a la compañía de haber recolectado mucha información durante el proceso de inscripción en el sitio, incluidos el domicilio y la contraseña del email del usuario. La FTC dijo que al recolectar las contraseñas de email – que no era algo que el negocio necesitara – y al guardarlas en un formato de texto sin codificación, la compañía generó un riesgo innecesario para las cuentas de email de la gente. El negocio podría haber evitado ese riesgo si en primer lugar no hubiera recolectado esa información delicada.

Retenga la información solo durante el tiempo que la necesite para un fin comercial legítimo.

A veces es necesario recolectar datos personales como parte de una transacción. Pero puede ser imprudente conservar esos datos después de cerrada la transacción. En el caso de la FTC contra ***BJ's Wholesale Club***, se alegó que la compañía recolectó los datos de las tarjetas de crédito y débito de los clientes para procesar las transacciones en sus tiendas minoristas. Pero de acuerdo a los términos de la demanda, continuó almacenando los datos durante 30 días – bastante tiempo después de la fecha de venta. La FTC dijo que lo que hizo BJ's Wholesale Club no solo infringió las regulaciones

bancarias, sino que la retención de la información sin una necesidad comercial legítima también generó un riesgo injustificado. Aprovechándose de las debilidades de las prácticas de seguridad de la compañía, unos piratas informáticos robaron los datos y los usaron para falsificar tarjetas de crédito y débito. El negocio podría haber limitado su riesgo eliminando la información financiera de manera segura cuando ya no tenía una necesidad legítima de conservarla.

No use información personal cuando no sea necesario.

Usted no haría malabares con un jarrón Ming. Su negocio tampoco debería usar información personal en contextos donde se puedan generar riesgos innecesarios. En el caso ***Accretive***, la FTC alegó que la compañía usó información personal verídica en sus sesiones de capacitación de empleados, y que omitió eliminar la información de las computadoras de los empleados después de finalizadas las sesiones. De manera similar, en el caso ***foru International***, la FTC acusó a la compañía de facilitar el acceso a datos delicados de los consumidores a unos proveedores de servicio que estaban desarrollando aplicaciones para la compañía. En ambos casos, se podría haber evitado ese riesgo usando información ficticia tanto para propósitos de capacitación de empleados como para el desarrollo de las aplicaciones.

2 Controle prudentemente el acceso a los datos.

Una vez que haya decidido que tiene una necesidad comercial legítima que justifica la retención de datos delicados, tome las medidas lógicas para protegerlos. Por supuesto que deberá mantener la información a salvo de la mirada indiscreta de los extraños. ¿Pero qué sucede con sus propios empleados? No todos los integrantes de su personal necesitan acceder de manera irrestricta a su red y a su información. Implemente controles para que sus empleados puedan acceder a la red únicamente sobre un criterio de una “necesidad de conocer los datos”. Para proteger su red informática, considere adoptar medidas tales como establecer cuentas de usuario separadas para limitar el acceso a los archivos donde se almacenan los datos personales o para controlar quiénes pueden usar bases de datos en particular. Para los archivos de papel, discos externos, otros dispositivos de almacenamiento de archivos, etc., el control del acceso podría ser algo tan simple como instalar un archivero con llave. Al momento de pensar en cómo controlar el acceso a la información delicada que tiene en su poder, considere estas lecciones que surgen de los casos de la FTC.

Restrinja el acceso a los datos delicados.

Si los empleados no tienen que usar información personal como parte de su trabajo, entonces no es necesario que tengan acceso a esos datos. Por ejemplo, en el caso ***Goal Financial***, la FTC alegó que la compañía no restringió el acceso de sus empleados para

evitar que accedieran a la información personal almacenada en sus archivos impresos y en su red informática. En consecuencia, un grupo de empleados transfirió más de 7,000 archivos de consumidores con información delicada a personas ajenas a la compañía. La compañía podría haber prevenido este error implementando controles adecuados y tomando las medidas necesarias para asegurarse de que solo aquellos empleados autorizados que tuvieran una necesidad comercial pudieran acceder a la información personal de la gente.

Limite el acceso a los controles administrativos del sistema.

El acceso a los controles administrativos, que es lo que permite que un usuario efectúe amplios cambios en su sistema, debería estar limitado al empleado a cargo de esa tarea. Por ejemplo, en su acción contra ***Twitter***, la FTC alegó que la compañía les otorgó acceso de control administrativo sobre el sistema de Twitter a casi todos sus empleados, incluso con la posibilidad de restablecer las contraseñas de las cuentas de los usuarios, ver los tweets privados de los usuarios, y enviar tweets en nombre de los usuarios. Según se alegó en la demanda, otorgándole acceso administrativo a casi todos sus empleados, Twitter aumentó el riesgo de que la exposición de las credenciales de cualquiera de sus empleados pudiera dar lugar a un incidente grave de seguridad de datos. ¿Qué podría haber hecho la compañía para reducir ese riesgo? Tomar medidas para asegurar que el acceso de los empleados a los controles administrativos del sistema estuviera adaptado a las necesidades de sus tareas.

3 Exija el uso de contraseñas seguras y un procedimiento de autentificación.

Si usted archiva información personal en su red informática, la implementación de sólidos procedimientos de autentificación – incluida una regla clara y firme para el establecimiento de contraseñas – puede ayudarlo a garantizar que solo aquellos individuos autorizados puedan acceder a los datos. Cuando desarrolle las políticas de su compañía puede considerar algunas de las recomendaciones que surgen de los casos de la FTC.

Insista en la creación de contraseñas únicas y complejas.

Establecer “contraseñas” como 121212 o qwerty no ofrece mucha más protección que ninguna contraseña en absoluto. Por lo cual, es prudente que analice los estándares a implementar para la creación de las contraseñas. Por ejemplo, en el caso ***Twitter***, la compañía permitió que sus empleados crearan contraseñas de control administrativo con palabras que comúnmente figuran en los diccionarios, y también les permitió usar las mismas contraseñas que estaban usando en otras cuentas. Según la FTC, esas prácticas laxas generaron una vulnerabilidad en el sistema de Twitter que fue aprovechada por unos piratas informáticos que usaron herramientas de predicción de contraseñas, o que

trataron de acceder usando contraseñas robadas a otros servicios esperando que los empleados de Twitter hubieran usado la misma contraseña para acceder al sistema de la compañía. Twitter podría haber evitado esos riesgos implementando un sistema de contraseñas más seguro – por ejemplo, exigiéndole a sus empleados que escogieran contraseñas complejas y capacitándolos para que no usaran la misma contraseña o una similar para acceder a las cuentas comerciales y a las cuentas personales.

Guarde las contraseñas de manera segura.

No les facilite el acceso a las contraseñas a los intrusos. En el caso ***Guidance Software***, la FTC alegó que la compañía almacenó credenciales de usuario de la red en un formato de texto sin codificar legible que facilitó un acceso pirata a la información de tarjeta de crédito de los clientes que estaba almacenada en la red. De manera similar, en el caso ***Reed Elsevier***, la FTC alegó que el negocio permitió que los clientes almacenaran en sus computadoras credenciales de usuario en cookies de formato vulnerable. También en el caso de ***Twitter***, la FTC dijo que la compañía no estableció políticas para prohibirles a sus empleados el almacenamiento de contraseñas administrativas en formato de texto sin codificación para las cuentas personales de email. En ambos casos, las compañías podrían haber reducido los riesgos implementado políticas y procedimientos para almacenar las credenciales de manera segura. También es conveniente que los negocios consideren otras protecciones – por ejemplo, un sistema de doble autentificación – que puede ser útil para proteger las contraseñas.

Establezca una protección contra los ataques de fuerza bruta.

¿Recuerda aquel dicho sobre el experimento con una cantidad infinita de monos operando una cantidad infinita de máquinas de escribir? Los piratas informáticos usan programas automatizados que realizan una función similar. Estos ataques de fuerza bruta consisten en el ingreso de interminables combinaciones de caracteres hasta que los piratas informáticos logran dar con la contraseña de alguna persona. En los casos de ***Lookout Services***, ***Twitter*** y ***Reed Elsevier***, la FTC alegó que los negocios no suspendieron ni deshabilitaron las credenciales de los usuarios después de cierta cantidad de intentos frustrados de acceso a las cuentas. Al no restringir adecuadamente la cantidad de intentos, las compañías pusieron en riesgo sus redes. Las compañías podrían haber eliminado ese riesgo implementado una política que suspendiera o deshabilitara las cuentas después de repetidos intentos de acceso.

Establezca una protección para que no se pueda circunvalar el paso de autentificación.

Cerrar con llave la puerta principal no ofrece demasiada protección si se deja abierta la puerta trasera. En el caso ***Lookout Services***, la FTC alegó que la compañía no probó adecuadamente su aplicación web para verificar si era vulnerable a fallos de seguridad ampliamente conocidos, incluido un fallo llamado “locación predecible de recursos”. En

consecuencia, un pirata informático pudo predecir fácilmente los modelos y manipular las URL para puentear la pantalla de autentificación de la aplicación web y acceder a las bases de datos de la compañía sin la debida autorización. La compañía podría haber aumentado el nivel de seguridad de su mecanismo de verificación probando las vulnerabilidades más comunes.

4 Archive la información personal delicada de manera segura y protéjala durante la transmisión.

Muchas compañías tienen una necesidad comercial que justifica el almacenamiento de datos delicados. Y aunque usted tome las medidas apropiadas para proteger su red informática, a veces tiene que enviar los datos a otra parte. Use una codificación sólida para proteger el material confidencial durante el proceso de almacenamiento y transmisión. El método a aplicar dependerá de los tipos de información que recolecte su negocio, y de cómo la recolecte y la procese. Dependiendo de la naturaleza de su negocio, algunas alternativas podrían ser el sistema de codificación TLS/SSL (Transport Layer Security/Secure Sockets Layer), codificación de datos inactivos o un código criptográfico iterativo. Pero cualquiera que sea el método que elija, solo funcionará correctamente si el personal que lo implementa lo hace de la manera apropiada. Controle que el personal asignado a esta tarea comprenda el modo en que su compañía usa los datos delicados y tenga los conocimientos necesarios para determinar qué es lo que debe hacer en cada situación. Considerando esos conceptos, estas son algunas lecciones que surgen de los casos de la FTC que usted debe tener en cuenta cuando tome medidas para proteger la información delicada durante el proceso de almacenamiento y transmisión.

Mantenga la seguridad de la información delicada a lo largo de su vida útil.

Los datos no permanecen quietos en un lugar. Por lo cual, si su negocio necesita transmitir información, es importante que considere la seguridad en todas las etapas. Por ejemplo, en el caso ***Superior Mortgage Corporation***, la FTC alegó que la compañía usó codificación SSL para proteger la transmisión de la información delicada entre el navegador de internet del cliente y el servidor del sitio web del negocio. Pero cuando la información llegó al servidor, el proveedor de servicio de la compañía la decodificó y la envió por email a la oficina central y a las sucursales de la compañía en un formato de texto legible y sin codificación. La compañía podría haber prevenido ese riesgo verificando la protección de los datos a lo largo de su vida útil, y no solo durante la transmisión inicial.

Use métodos probados y aceptados por la industria.

Cuando esté considerando los estándares técnicos a seguir, tenga presente que es posible que los expertos ya hayan desarrollado estándares efectivos que usted puede aplicar en su negocio. Las compañías inteligentes no comienzan el proceso desde cero cuando no es necesario. En lugar de eso, aprovechan los conocimientos de los expertos. El caso ***ValueClick*** ilustra ese principio. Según la FTC, la compañía almacenó información delicada de clientes que había sido recolectada a través de sus sitios de e-commerce en una base de datos con un formato de codificación no convencional de su propiedad. En la demanda se alegó que en lugar de usar una codificación de algoritmos ampliamente aceptada y exhaustivamente probada, ValueClick usó un método que consistía en un sistema simple de sustitución alfabética sujeto a importantes vulnerabilidades. La compañía podría haber evitado esas debilidades usando métodos de protección de datos de probada efectividad y aceptados por el sector.

Controle la correcta configuración del sistema de codificación.

La codificación – incluso los métodos más sólidos – no les ofrecerá protección a sus usuarios si usted no la configura correctamente. Ese es un mensaje que los negocios pueden extraer de las acciones de la FTC contra ***Fandango*** y ***Credit Karma***. En estos casos, la FTC alegó que las compañías usaron una codificación SSL en sus aplicaciones móviles, pero que desactivaron un proceso crítico conocido como validación del certificado SSL sin implementar ninguna otra medida compensatoria de seguridad. Eso causó la vulnerabilidad de las aplicaciones a los ataques de intermediarios que permitió que los piratas informáticos decodificaran la información delicada transmitida por las aplicaciones. La compañía podría haber prevenido esos riesgos configurando correctamente las implementaciones del sistema de codificación SSL.

5 Segmente su red y haga un monitoreo para controlar quién está tratando de entrar y salir.

Cuando diseñe su red informática, considere utilizar algunas herramientas como los firewalls para segmentarla, de ese modo podrá limitar el acceso entre las computadoras de su red y entre sus computadoras e internet. Otra protección útil: las herramientas de detección y prevención para monitorear la actividad maliciosa en su red informática. Estas son algunas lecciones que surgen de los casos de la FTC a tener en cuenta cuando diseñe su red.

Segmente su red.

No es necesario que todas las computadoras de su sistema se puedan comunicar con cada computadora de su compañía. Usted puede proteger los datos particularmente delicados alojándolos en un lugar seguro y separado de su red. Esa es una lección

que surge del caso ***DSW***. La FTC alegó que la compañía no limitó adecuadamente la red informática de una de sus tiendas para evitar que las computadoras se conectaran con otras redes de sus tiendas y de la sede de la compañía. En consecuencia, los piratas informáticos pudieron usar la red de una tienda para conectarse y acceder a la información de las redes de otras tiendas y de la sede de la compañía. La compañía podría haber reducido ese riesgo segmentando adecuadamente su red informática.

Monitoree la actividad de su red informática.

"¿Quién está golpeando a mi puerta?" Eso es lo que pregunta una herramienta de detección de intrusión efectiva cuando detecta una actividad no autorizada en su red. En el caso ***Dave & Buster's***, la FTC alegó que la compañía no usó un sistema de detección de intrusiones y no monitoreó la actividad sospechosa de los registros del sistema. La FTC dice que en el caso ***Cardsystem Solutions*** sucedió algo similar. El negocio no implementó las medidas adecuadas para detectar el acceso no autorizado a su red. Los piratas informáticos se aprovecharon de esa debilidad del sistema e instalaron programas en la red de la compañía mediante los cuales pudieron recolectar datos delicados y continuar enviándolos fuera de la red cada cuatro días. En cada uno de estos casos, los negocios podrían haber reducido el riesgo de una exposición de datos o el alcance del incidente usando herramientas para monitorear las actividades de sus respectivas redes informáticas.

6 Proteja el acceso remoto a su red informática.

La actividad de un negocio no se desarrolla únicamente en la oficina. Si bien es cierto que tener personal que realiza tareas fuera de la oficina puede aumentar la productividad de su negocio, también es cierto que la movilidad puede plantear nuevos desafíos para la seguridad. Si usted permite que sus empleados, clientes o proveedores de servicio accedan a su red informática desde terminales remotas, ¿ha tomado las medidas necesarias para proteger esos puntos de acceso? Los casos de la FTC indican algunos factores a tener en cuenta cuando desarrolle sus políticas de acceso remoto.

Controle la seguridad en cada terminal de acceso.

Así como la fortaleza de una cadena se define por su eslabón más débil, el nivel de seguridad de su red estará determinado por la computadora más vulnerable con acceso remoto a su red. Ese es el mensaje de los casos de la FTC contra unas compañías que no tomaron las medidas de seguridad necesarias para proteger las terminales con acceso remoto a sus redes. Por ejemplo, en el caso ***Premier Capital Lending***, la compañía presuntamente habilitó una sesión de conexión a una cuenta para que un cliente del negocio pudiera obtener informes de consumidores sin evaluar previamente la seguridad de ese cliente. Cuando los piratas informáticos accedieron al sistema del

cliente, le robaron sus credenciales de conexión remota y las usaron para apropiarse de la información personal de los consumidores. De acuerdo a la demanda contra ***Settlement One***, el negocio permitió que algunos clientes que carecían de las medidas básicas de seguridad, como firewalls y software antivirus actualizado, accedieran a informes de consumidores a través de su portal en línea. Y en el caso ***Lifelock***, la FTC alegó que la compañía no instaló programas antivirus en las computadoras que los empleados usaban para acceder remotamente a su red informática. Estos negocios podrían haber reducido esos riesgos protegiendo las computadoras con acceso remoto a sus redes.

Implemente límites prudentes para el acceso.

No todas las personas que ocasionalmente pudieran tener la necesidad de acceder a su red deben tener un pase libre para acceder a toda la información confidencial. Por lo cual, es prudente limitar el acceso solo a aquellos datos necesarios para realizar la tarea. Por ejemplo, en el caso ***Dave & Buster's***, la FTC alegó que la compañía no restringió adecuadamente el acceso de terceros a su red. Aprovechando la debilidad del sistema de una tercera compañía, presuntamente, un intruso logró conectarse a la red varias veces e interceptar información personal. ¿Qué podría haber hecho la compañía para reducir ese riesgo? Podría haber implementado límites para evitar el acceso de terceros a su red – por ejemplo, restringiendo las conexiones a domicilios IP especificados o concediendo un acceso temporario y limitado.

7 Aplique prácticas de seguridad sólidas al desarrollo de nuevos productos.

En su tablero de diseño usted tiene una gran aplicación nueva o un software innovador. En las primeras etapas del proceso de desarrollo piense cómo les gustaría usar el producto a los clientes. Si los clientes van a almacenar y enviar información delicada, pregúntese si su producto está en condiciones de manejar los datos de manera segura. Antes de lanzar su producto al mercado, considere las lecciones de los casos de la FTC relacionados con desarrollo, diseño, prueba y puesta en marcha de un producto.

Capacite a sus ingenieros en materia de codificación de seguridad.

¿Les ha explicado a sus desarrolladores la necesidad de mantener la seguridad en primera línea? En los casos de ***MTS***, ***HTC America***, y ***TRENDnet***, la FTC alegó que las compañías no capacitaron a sus empleados en materia de prácticas de codificación seguras. El resultado: decisiones de diseño cuestionables, incluso la introducción de vulnerabilidades en el software. Por ejemplo, según la demanda del caso ***HTC America***, la compañía no implementó mecanismos de comunicación segura fácilmente disponibles en la fase de inicio de sesión de las aplicaciones preinstaladas en sus aparatos móviles.

En consecuencia, unas aplicaciones maliciosas de terceros pudieron comunicarse con las aplicaciones de inicio de sesión, poniendo en riesgo los mensajes de texto, datos de localización y otra información delicada de los consumidores. La compañía podría haber reducido el riesgo de ese este tipo de vulnerabilidades capacitando adecuadamente a sus ingenieros en materia de prácticas de codificación seguras.

Siga las pautas de plataformas de seguridad.

En lo que se refiere a la seguridad, tal vez no sea necesario reinventar la rueda. A veces, la opción más prudente es escuchar a los expertos. En las acciones entabladas contra ***HTC America***, ***Fandango*** y ***Credit Karma***, la FTC alegó que las compañías no siguieron las pautas explícitas de las plataformas sobre las prácticas de desarrollo seguras. Por ejemplo, Fandango y Credit Karma desactivaron en sus aplicaciones un proceso crítico de validación de certificados llamado SSL, permitiendo que la información delicada de los consumidores se retransmitiera por medio de esas aplicaciones que estaban abiertas a la intercepción a través de ataques de intermediarios. Las compañías podrían haber prevenido esta vulnerabilidad siguiendo las pautas de iOS y Android para desarrolladores, que advierten explícitamente contra la desactivación de la validación de certificados SSL.

Verifique el correcto funcionamiento de las funciones de privacidad y seguridad.

Si su software le ofrece una función de privacidad o seguridad, verifique que esa función opere tal como se anuncia. Por ejemplo, en el caso ***TRENDnet***, la FTC acusó a la compañía de no probar la efectividad de una opción para mantener la privacidad de las filmaciones de las cámaras de los consumidores para restringir el acceso a esas filmaciones. En consecuencia, cientos de filmaciones privadas quedaron a la vista del público. De manera similar, en el caso ***Snapchat***, la compañía anunció que los mensajes “desaparecerían para siempre”, pero la FTC dice que la compañía no tomó las medidas necesarias para garantizar la veracidad de esa declaración. Entre otras cosas, la aplicación almacenó archivos de video fuera del entorno restringido de verificación o sandbox de la aplicación, facilitando la recuperación de los archivos de video con herramientas comunes de visualización de archivos. Lecciones que surgen de los casos de otras compañías: cuando ofrezca funciones de privacidad y seguridad, controle que su producto funcione conforme a sus declaraciones publicitarias.

Pruebe las funciones para detectar las vulnerabilidades comunes.

No hay manera de prever cada amenaza, pero hay algunas vulnerabilidades que son comúnmente conocidas y lógicamente evitables. En más de una docena de casos de la FTC, los negocios no evaluaron adecuadamente sus aplicaciones para verificar la existencia de vulnerabilidades bien conocidas. Por ejemplo, en el caso ***Guess?***, la FTC alegó que el negocio no evaluó si su aplicación web era vulnerable a los ataques por

inyección SQL (Structured Query Language). En consecuencia, los piratas informáticos pudieron usar ataques SQL para acceder a bases de datos que contenían información de tarjeta de crédito de consumidores. Ese es un riesgo que se podría haber evitado probando las vulnerabilidades comúnmente conocidas, como aquellas identificadas en el Open Web Application Security Project (OWASP) (enlace externo).

8 Controle que sus proveedores de servicio implementen medidas de seguridad lógicas.

En materia de seguridad, abra bien los ojos para mantener vigilados a sus proveedores de servicio – por ejemplo, las compañías que contrata su negocio para procesar la información personal de sus clientes o para desarrollar aplicaciones. Antes de contratar un proveedor, sea franco respecto a sus expectativas de seguridad. Siga los pasos lógicos y necesarios para seleccionar proveedores capaces de implementar medidas de seguridad adecuadas y para controlar que acaten sus requerimientos. Los casos de la FTC ofrecen consejo sobre lo que se debe tener en cuenta al momento de contratar y supervisar a los proveedores de servicios.

Póngalo por escrito.

Insista para que los estándares de seguridad apropiados formen parte de sus contratos. Por ejemplo, en el caso ***GMR Transcription***, la FTC alegó que la compañía contrató proveedores de servicio para transcribir archivos de audio con información delicada, pero omitió exigirle al proveedor del servicio que tomara medidas de seguridad lógicas. En consecuencia, los archivos – muchos de ellos con datos de salud altamente confidenciales – quedaron ampliamente expuestos en internet. Por empezar, el negocio podría haber incluido disposiciones contractuales que les exigieran a los proveedores de servicio que adoptaran precauciones lógicas de seguridad, por ejemplo, un sistema de codificación.

Verifique el cumplimiento.

La seguridad no puede ser algo que se base en un “le doy mi palabra”. Un primer paso importante es incluir sus expectativas de seguridad en los contratos con sus proveedores de servicio, pero también es importante desarrollar tareas de supervisión a lo largo del proceso. El caso ***Upromise*** ilustra este punto. La compañía contrató un proveedor de servicio para desarrollar una barra de herramientas para un navegador. Upromise dijo que la barra de herramienta, que recolectaba información de navegación de consumidores para ofrecer ofertas personalizadas, usaría un filtro para “eliminar cualquier información personal identificable” antes de la transmisión. Pero según la FTC, Upromise omitió verificar que el proveedor de servicio hubiera implementado el programa de recolección de información de una manera coherente con las políticas de

privacidad y seguridad de Upromise y conforme a los términos del contrato diseñados para proteger la información de los consumidores. En consecuencia, la barra de herramientas recolectó información personal delicada, incluso números de cuentas financieras y códigos de seguridad de páginas web seguras, y los transmitió en formato de texto sin codificación. ¿Qué podría haber hecho la compañía para reducir ese riesgo? Hacerle preguntas al proveedor del servicio e implementar un seguimiento durante el proceso de desarrollo.

9 Implemente procedimientos para mantener actualizada su seguridad y ocúpese de solucionar las vulnerabilidades que pudieran surgir.

La protección de su software y de su red informática no es algo que se haga de una vez y para siempre. Es un proceso continuo que exige mantener la guardia alta. Si su red usa un software de terceros, o si sus aplicaciones incluyen bibliotecas de software de terceros, aplique actualizaciones a medida que estén disponibles. Si usted desarrolla su propio software, ¿qué medidas va a implementar para que la gente le informe si detectó una vulnerabilidad y qué hará usted para resolver el problema? Los casos de la FTC ofrecen algunos puntos a considerar al momento de analizar el manejo de las vulnerabilidades.

Actualice y repare el software de terceros.

Un software desactualizado atenta contra la seguridad. La solución es actualizarlo regularmente e implementar los parches de terceros. Por ejemplo, en el caso ***TJX Companies***, la FTC alegó que la compañía no actualizó su software antivirus, aumentando el riesgo de que los piratas informáticos pudieran explotar las vulnerabilidades o vencer las defensas del negocio. Dependiendo de la complejidad de su red informática o de su software, es posible que tenga que priorizar los parches de acuerdo a su nivel de gravedad; no obstante, una medida importante para reducir el riesgo de una exposición de datos es implementar un proceso lógico para actualizar y reparar los programas de terceros.

Preste atención a las advertencias de seguridad y actúe rápidamente para solucionarlas.

Cuando se presenten vulnerabilidades, escuche atentamente y actúe. En el caso ***HTC America***, la FTC alegó que la compañía no tenía implementado un proceso para recibir y ocuparse de los reportes de vulnerabilidades de seguridad. Presuntamente, la demora de HTC en responder a las advertencias implicó que las vulnerabilidades afectaran más aparatos a través de múltiples versiones del sistema operativo. A veces las compañías reciben alertas de seguridad, pero se pierden en la confusión. Por

ejemplo, en el caso ***Fandango***, la compañía confió en su sistema general de servicio al cliente para responder a las advertencias sobre los riesgos de seguridad. Según la demanda, cuando un investigador se comunicó con el negocio para reportar una vulnerabilidad, el sistema categorizó el reporte incorrectamente como una solicitud de restablecimiento de contraseña, envió una respuesta automática, y marcó el mensaje como "resuelto" sin marcarlo para su posterior revisión. En consecuencia, Fandango no se enteró de la vulnerabilidad hasta que el personal de la FTC se comunicó con la compañía. ¿Lecciones que surgen de otros negocios? Implemente un proceso efectivo para recibir y resolver los reportes de vulnerabilidad. Considere implementar un canal efectivo y claramente anunciado (por ejemplo, un domicilio de email exclusivo para ese fin como security(@)yourcompany.com) para recibir los reportes y marcarlos para que su personal de seguridad los revise.

10 Guarde en un lugar seguro los archivos de papel y los medios y dispositivos de almacenamiento.

La seguridad de la red es una consideración crítica, pero muchas de las mismas lecciones se aplican a la información impresa y a otros medios físicos de almacenamiento de información como discos duros, computadoras portátiles, unidades de memoria flash y discos de almacenamiento. Los casos de la FTC ofrecen elementos a considerar al momento de evaluar la seguridad física en su negocio.

Guarde los archivos con información delicada en un lugar seguro.

Si necesita retener documentación importante, tome medidas para protegerla. En el caso ***Gregory Navone***, la FTC alegó que el demandado guardó información delicada de consumidores que había recolectado en su ex negocio en unas cajas que mantuvo en su garaje. En la demanda del caso ***Lifelock***, se alegó que la compañía dejó documentos enviados por fax que contenían información personal de consumidores en un lugar abierto y de fácil acceso. En ambos casos, los negocios podrían haber reducido el riesgo para sus clientes implementado políticas para almacenar los documentos de manera segura.

Proteja los aparatos que procesan información personal.

Las medidas de seguridad que implemente para proteger la información almacenada en su red no servirán para proteger a sus clientes si los datos ya han sido robados a través del aparato o dispositivo que los recolecta. En 2007, en la investigación del caso ***Dollar Tree***, el personal de la FTC dijo que los dispositivos que el negocio utilizó para ingresar los números de identificación personal o PIN de los clientes eran vulnerables a la manipulación y al robo. En consecuencia, a través de un ataque conocido como "PED

skimming" unas personas no autorizadas pudieron capturar los datos de las tarjetas de pago de los consumidores, incluidos los datos de la banda magnética y el PIN. En ese momento, debido a lo novedoso de ese tipo de tentativa y a otros varios factores, el personal de la FTC cerró la investigación. Sin embargo, actualmente los ataques contra los dispositivos utilizados en los puntos de venta son bien conocidos y los negocios deben tomar las medidas lógicas y necesarias para proteger ese tipo de aparatos.

Implemente estándares de seguridad para proteger los datos itinerantes.

Los negocios inteligentes comprenden la importancia de proteger la información delicada mientras está fuera de la oficina. Por ejemplo, en el caso ***Accretive***, la FTC alegó que un empleado dejó su computadora portátil con más de 600 archivos que incluían 20 millones de datos relacionados con 23,000 pacientes dentro del compartimiento cerrado del asiento del pasajero de un automóvil que fue robado. El caso ***CBR Systems*** involucró cintas de copias de seguridad supuestamente codificadas, una computadora portátil y un disco externo – que contenían información delicada – que fueron sustraídos del automóvil de un empleado. En ambos casos, los negocios podrían haber reducido el riesgo para la información personal de los consumidores implementando políticas de seguridad lógicas para proteger los datos itinerantes. Por ejemplo, cuando envíe archivos, discos, unidades de memoria, etc., use un método que le permita hacer un seguimiento del trayecto del paquete. Limite las situaciones que impliquen que sus empleados salgan de la oficina con datos delicados en su poder. Pero cuando se presente una necesidad comercial legítima de viajar con información personal, los empleados la tienen que mantener fuera de la vista de terceros, y en la medida de lo posible, deben guardarla bajo llave.

Elimine los datos delicados de manera segura.

La documentación o los aparatos que ya no necesita le pueden parecer basura, pero si contienen información personal sobre consumidores o empleados, son un tesoro para los ladrones de identidad. Por ejemplo, de acuerdo a lo que se alega en las demandas de la FTC en los casos ***Rite Aid*** y ***CVS Caremark***, las compañías desecharon información personal delicada – como recetas de medicamentos – en contenedores de basura. En el caso ***Goal Financial***, la FTC alegó que un empleado vendió un excedente de discos duros que contenían información personal delicada de aproximadamente 34,000 clientes en formato de texto sin codificación. Las compañías podrían haber prevenido el riesgo para la información personal de los consumidores triturando, quemando o pulverizando los documentos para que quedaran ilegibles y usando tecnología disponible para borrar la información de dispositivos en desuso.

PARA MÁS INFORMACIÓN?

Puede encontrar más información en **ftc.gov/business** en la sección de Seguridad de Datos (en inglés).

ACERCA DE LA FTC

La FTC trabaja a favor del consumidor para prevenir las prácticas comerciales fraudulentas, engañosas y desleales en el mercado y para proveer información a los negocios para ayudarlos a cumplir la ley. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite **ftc.gov/español** o llame sin cargo al (1-877-382-4357); TTY: 1-866-653-4261. Para más información, mire el video Cómo presentar una queja ante la FTC en **consumidor.ftc.gov/media**. La FTC ingresa las quejas presentadas por los consumidores a una base de datos segura y herramienta investigativa llamada Red Centinela del Consumidor que es utilizada por cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y del extranjero.

SU OPORTUNIDAD DE PRESENTAR COMENTARIOS

La agencia National Small Business Ombudsman y 10 juntas regionales llamadas Regional Fairness Boards recogen comentarios de parte de las pequeñas empresas sobre las acciones federales de cumplimiento y fiscalización. Todos los años, el programa de defensa de la pequeña empresa evalúa la conducta de dichas actividades y califica la capacidad de respuesta de cada agencia ante las pequeñas empresas. Los representantes de las pequeñas empresas pueden presentar comentarios ante el Ombudsman sin temor a represalias. Para presentar comentarios, llame a la línea gratuita 1-888-REGFAIR (1-888-734-3247) o visite **sba.gov/ombudsman**.

La Comisión Federal de Comercio
business.ftc.gov
Junio 2015