SECURITY

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**, it's critical to know what personal information you have stored physically and electronically, and keep only what is essential for your business. Protect the information you keep, and properly dispose of what you no longer need. And, of course, create a plan to respond to security incidents.

The FTC also has *cybersecurity resources* especially for small businesses, including publications to address particular data security challenges, business alerts, 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 80 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.

Business executives often ask how to manage confidential information ranging from personal data on employment applications to network files with customers’ credit card numbers. Experts agree on the key first step: Start with security. Factor it into the decision-making 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. Instead, deliberately think through the implications of your 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

in **BLU**, the FTC alleged the company didn't impose limits on the consumer information that one of its contractors could access. The contractor collected and transferred to its servers far more information than it needed to do its job, including the full content of consumers' text messages, real time location data, call and text message logs with full telephone numbers, and contact lists. The company could have protected this sensitive consumer data by implementing appropriate security procedures to oversee the security practices of its service providers, as well as by ensuring that only authorized employees or contractors with a legitimate business need had access to users' personal information.

The FTC's complaint in **MoviePass** alleged the company failed to protect its users' personal and financial information, including by storing this information in plain text and then by failing to impose restrictions on who could access the data. MoviePass stored consumer information, including names, email addresses, birth dates, credit card numbers, and geolocation information. The company then loaded the information onto a server on which it had disabled the firewall, leaving the data accessible to anyone with an internet connection. The resulting data breach could have been avoided by encrypting consumer data and by maintaining and managing security controls to protect and restrict access to that data.

Limit administrative access.

Administrative access, which lets a user make system-wide changes to your system, should be limited to the employees tasked with that job. In its action against**Uber**, for example, the FTC alleged the company failed to restrict access to systems based on employees' job functions, and allowed all programs and engineers to use a single Amazon Web Services (AWS) access key that gave full administrative privileges over all the company's data in the cloud storage service. As a result of this practice, when an engineer posted the key to a software development site, a malicious actor was able to use it to access the sensitive personal information of thousands of Uber drivers, including names and driver's license, bank account, and Social Security numbers.

3 Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password management – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are lessons 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. Give some thought to the password standards you implement. In the FTC's 2011 **Twitter** case, for example, the FTC alleged that 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.

In **Drizly**, the FTC alleged the company failed to require unique and complex passwords or multifactor authentication for accessing the company's GitHub repositories.
A Drizly executive reused a password he had used for other personal accounts, but his recycled password was exposed in an unrelated breach. This created an opportunity for a malicious actor to access Drizly's GitHub repositories, which made it possible for the attacker to access other database credentials and ultimately exfiltrate the personal information of 2.5 million consumers. The company could have reduced those risks by requiring that employees create unique and complex passwords (i.e., long passwords not used by the person for any other online service) or multifactor authentication to protect access to source code or databases. Even better, companies can require employees to use security keys for access.

Protect against authentication bypass.

Locking the front door doesn’t offer much protection if the back door is 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 include Transport Layer Security (TLS) 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 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, 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. Don't start from scratch when it isn't necessary. Instead, take advantage of collected wisdom. The **Lenovo** case illustrates that principle. According to the FTC, the company used an insecure method to replace digital certificates on encrypted websites with certificates signed by its own software. However, its software didn't adequately verify that the websites' digital certificates were valid before replacing them. The company could have avoided this weakness by using tried-and-true industry-tested and accepted methods for authenticating websites.

Ensure proper configuration.

Even the strongest encryption 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 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.

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

When designing your network, consider using tools to validate and limit implicit trust between networked systems. Assume that all traffic regardless of source is hostile. Part of your "zero trust" toolkit should be tools to inspect and log network traffic – like SIEM and SOAR tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Continuously validate access to data.

Not every computer in your system needs to be able to communicate with every other one. Help protect particularly sensitive data by housing it in a separate secure place on your network. That’s a lesson from the **Infotrax** case. The FTC alleged the company didn’t sufficiently limit one client’s distributors from accessing another client’s data on the network. As a result, hackers penetrated the company’s server through a single client’s website and could then access every client’s consumer data on the network. The company could have reduced that risk by continuously validating access to its data.

Monitor activity on your network.

“What’s happening on my network?” An effective SIEM tool will allow your security staff to answer that question.

In **i-Dressup**, the FTC alleged that the company didn’t use an intrusion detection and prevention system. After a hacker accessed the company’s computer network and compromised the personal information of about 245,000 children under the age of 13, the company learned of the breach only after hearing from a journalist who had been in contact with the hacker. The company could have detected this data breach much earlier by using readily available and low-cost security measures to alert them to instances of unauthorized access to their network.

More generally, in the **DealerBuilt** case, the FTC alleged the company didn’t use security measures to monitor its systems and assets. As a result, when an employee connected a storage device to the company’s backup network without ensuring it was securely configured, the resulting insecure connection created an opportunity for a hacker to breach the backup database. The FTC said that hacker then downloaded the personal information of tens of thousands of consumers, including their Social Security and driver’s license numbers, birth dates, and financial information. The company could have identified this breach sooner by using readily available tools to monitor its systems.

Security-centric companies may consider using “canaries” to help uncover unauthorized access attempts. What’s a canary? It’s a ruse designed to test if intruders are trying to get into your system without actually putting your network at risk. This could involve, for example, adding hardware or software to a mock network that doesn’t really interact with your system. If something does try to interact with it, that’s a sign you may have an intruder moving around your network.

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 > W S R > ^ P Y, the FTC charged that the company failed to install antivirus programs on the computers that employees used to access its network remotely. Businesses today could reduce these risks by using endpoint detection and response, as well as extended detection and response security solutions – often called EDR/XDR tools – to strengthen security of network endpoints and allow faster detection and response to security incidents.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should hentic.97-22.onsecurit gs /d

Verify compliance.

because its patch management policies and procedures were inadequate. Depending on the complexity of your network or software, you may need to prioritize patches by the severity of the threat they are designed to avert. Nonetheless, having a reasonable process in place to update and patch third-party software is an important step toward reducing the risk of a compromise. Consider using automated tools to track which versions of software your system is running and whether updates are available.

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 : F 4 2 \ R a W P M 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 7 M] Q M] U ^, 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 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**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 consumers’ payment card information, 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 numLr78 >>BDC EMC /P <</Lang (en-US)/MCID 5stoon /GecÞÎè ªüi".ÞÎîX ï•ree

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 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?

Visit the Data Security section of**business.ftc.gov** for a listing of relevant cases and other free resources.

About the FTC

The FTC works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers. Report scams and bad business practices at **ReportFraud.ftc.gov**. We also provide guidance at **business.ftc.gov** to help companies 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. Looking for a quick take on recent cases and other initiatives? Subscribe to the 7F4mb 3dbW]Rbb 3Z^U.

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

August 2023