partners bank of california

A GUIDE FOR BUSINESS

Start with Security

Introduction

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.

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 this guide, we'll cover 10 security principles that businesses should consider implementing.

A GUIDE FOR BUSINESS

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.

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 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. 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. There are benefits to 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? Avoid risk by simply 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. Limit risk by securely disposing of financial information once it no longer has a legitimate need for it.

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

You wouldn't juggle with a vase. Nor should businesses use personal information in contexts that create unnecessary risks. Risk can be avoided by using fictitious information for employee training sessions 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.

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. Implement proper controls and ensure that only authorized employees with a business need have 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. Ensure 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.

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. Limit risk 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. Risk can be reduced if companies have 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. Implementing a policy to suspend or disable accounts after repeated login attempts would help to eliminate risk.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is left open. Companies could improve the security of their authentication mechanisms 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.

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. Risk can be prevented by ensuring the data is 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. Companies can avoid 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. Risks can be prevented if companies' implementations of SSL have 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.

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. Companies can reduce 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. Businesses can reduce 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?

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. Businesses can reduce risk 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 allaccess, backstage pass. That’s why it’s wise to limit access to what’s needed to get the job done. Companies can place limits on third-party access to their 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?

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? Companies can reduce the risk of vulnerabilities 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. Companies can prevent vulnerability by following the iOS and Android guidelines for developers – for example, 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. 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. Risk can be 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.

Put it in writing.

Insist that appropriate security standards are part of your contracts. To avoid risk, businesses can include 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. Companies can reduce risk by asking questions and following up with service providers 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?

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. 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. 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.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. Businesses can reduce 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. Attacks targeting point-of-sale devices are 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. Businesses can reduce 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. Companies can prevent the risk to consumers' personal information by shredding, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

Looking for more information?

In addition to this guide, we offer a Identifying and Addressing BEC and Wire Fraud Attacks Guide, and Cybersecurity Guide. We also offer a free basic Risk Assessment to help your organization start an incident response plan to help identify, prevent and address cybersecurity-related attacks. Contact our Treasury Management team to obtain the self-assessment tool by email at tm@pbofca.com or by calling (949) 732-4050. The FTC's Business Center (business.ftc.gov) also has a Data Security section with free resources.

For additional information or questions about how to protect your company from cyberattacks, vist our Resource Center on pbofca.com or contact support@pbofca.com.

MISSION VIEJO

Corporate Headquarters
27201 Puerta Real, Suite 160
Mission Viejo, CA 92691

(949) 732-4000

BEVERLY HILLS

8484 Wilshire Blvd., Suite 520
Beverly Hills, CA 90211

(323) 556-6544

pbofca.com

Member FDIC
EQUAL HOUSING LENDER