A BIO-key® Solution.

White Paper

7 Best Practices for Improving Sensitive Data Security

Table of Contents

Table of Contents

Introduction

Summary

If the last few years have taught us anything about the digital environment, it is the precariousness of information security. Data breaches have gone from a periodic, randomly appearing nuisance for large corporations to a commonly occurring problem for the general population. The theft of sensitive data has been publicized so often that regular credit and identity theft checks have become standard practice for many everyday individuals.

Information security is seemingly slow to catch up to those who seem to know all too well that knowledge is power. Fortunately, there are many actions that can be taken to improve the security of sensitive data, and help prevent its loss from creating an opportunity for irrevocable damage. It all comes down to understanding the attackers, where they come from, and what they want.

In his widely praised work, **The Code Book**[i], Simon Singh continually builds to the argument that nothing is secure forever. The allusion speaks to the evolution of security and theft; that attackers - hackers, thief's and their ilk – will always find a way to circumvent security in one way or another. The point, however, is not to become discouraged by this seemingly eternal conflict, but rather to do whatever is necessary to stay ahead of the curve.

Understanding how to protect sensitive data from becoming compromised is the first step to take in an effort to reduce the likelihood of a data breach and a potentially ruinous loss to both finances and reputation. With technological advances moving forward at an ever-increasing pace, it has never been more important to know how to improve both internal and external security. Attackers show no signs of slowing up progress – neither should you.

This paper serves to establish a substantial definition for what is and what should be considered sensitive data, and a wide array of best practices to help keep that data secure.

Years of Data Breaches

Since 2014 many large corporations, such as JP Morgan Chase[ii], Home Depot[iii], and Sony Pictures[iv], were breached and had their private, corporate records stolen, exposed and/or manipulated for the profit of others and the detriment of those individuals involved. It doesn't appear that these issues are slowing down anytime soon. In 2017, data breach incidents reached a new record high, no thanks in part to the Equifax[v] data breach that affected 143 million individuals, and then rose to nearly 150 million by March 2018.

Compiling data from reports[vi] issued by the Identity Theft Resource Center, it is illustrated since 2014 that there has been a major upswing in data breaches across all verticals. What this illustrates is that current tactics for securing sensitive data are not working. While government and military occurrences have been reduced slightly, educational, banking and healthcare related breaches are still occurring at an alarming rate – putting even more of the general population at risk to lose everything.

This trend can be halted, however, through a more inclusive understanding of what sensitive data is, and how to better protect it from attackers – both external and within. Data is everywhere, and no matter the size of the company, or the industry, the last several years of data breaches have shown that any stolen information can wreak untold havoc.

What is Sensitive Data?

Sensitive data can mean many things to many different people. For credit card holders and bankers, sensitive data refers to account information, card numbers, and identity. For teachers, sensitive data can refer to specific personal information, such as home addresses, social security numbers, or even student information. Individual organizations or companies might refer to sensitive data as corporate secrets or payroll information – or an entire host of other bits of data that could potentially be used against the company or the individual.

What all of these scenarios have in common is that sensitive data is specific to the conditions in which it exists. Understanding the extent to which some information needs to be protected will require an in-depth evaluation of the environment in question.

If you are worried about your data, you need to establish a clear organization for said data, and educate your employees and/or end-users on this organization.

Typical organization falls into three categories:

- Restricted Data
- Private/Con-dential Data
- Publicly Accessible Data

Once this organization is established, analyzed and understood beyond reproach, you will have a much more sophisticated understanding of what information needs securing, and what direction to take in order to achieve that goal.

Here are our top best practices for securing that sensitive data in the best, most effective way possible.

Best Practices for Improving Sensitive Data Security

These best practices have been broken up into the following four categories based on overall similarities in purpose and function to secure data:

- Integration
- Implementing a Central Filter
- Multifactor Authentication
- Strong Password Policies

Integration

Secure Portal Access

Integrating a secure portal into your digital environment serves as a strong gateway to segment your categorized data. One of the most important rules in securing sensitive data is to make sure that access to publicly accessible data and private, confidential data is completely and distinctly separated. A secure portal makes this task simple and provides you with a much higher level of control over who has access to what information.

Additionally, secure portal integration can be made to blend completely with your existing environment, while some third-party software will standout in an obvious manner – increasing user frustration and the likelihood of engendering mistrust. Clear, consistent branding serves to improve user experience as well as mitigate unwanted, potentially threatening workarounds that end users may take to obtain the desired resources/information.

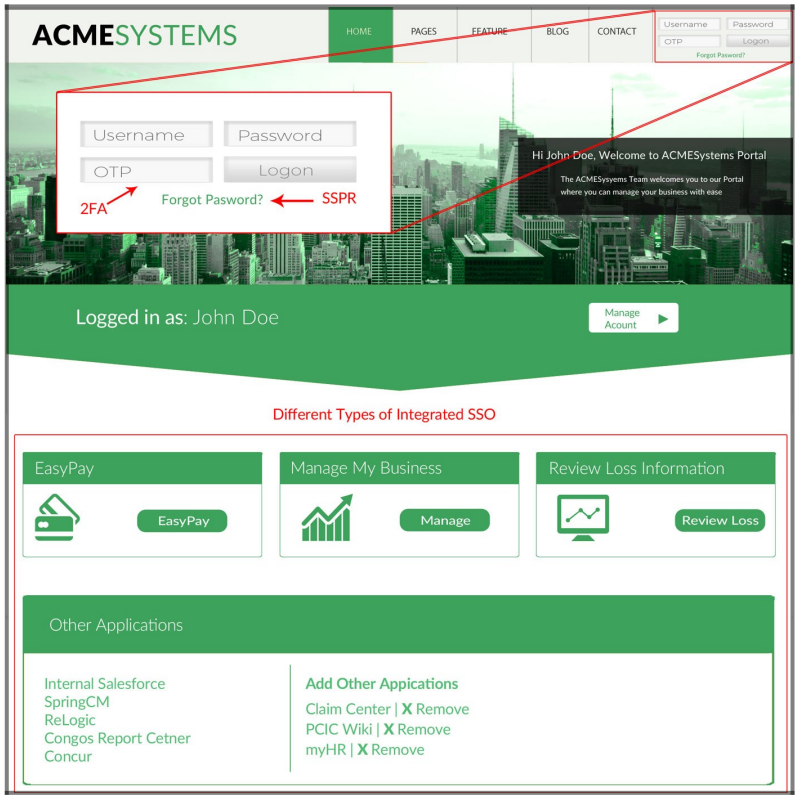
Single Sign-On

The modern workplace environment requires users to navigate through several different web applications with individual login prompts and requirements of their own. Such tedious behavior detracts from the user experience, and can potentially place the user at risk of being the subject of a man-in-the-middle attack or other in-transit data theft. Single Sign-On integration relies heavily on the implementation and adherence to industry standard protocols for continuously up-to-date security and protection of data in-transit from the identity provider to the service provider in question.

Such adherence adds an invisible layer of security to login credentials and mitigates the threat of exposing the internal network to potentially unsafe traffic to and from less-secure web applications.

Additionally, Single Sign-On reduces the likelihood of user passwords being compromised due to lost or forgotten passwords by requiring the user to remember only one set of credentials for access to all of his or her necessary applications. Users are much more likely to create and remember a single, strong password than they are to remember multiple passwords that require a higher level of complexity.

One point of caution is that Single Sign-On is not a silver bullet. Certain styles of SSO such as identity federation are supported only by code existing on both the target site and the website vouching for the user's identity. This code can have bugs or vulnerabilities that require updates. For example, a serious SAML vulnerability was discovered in February 2018[vii].



Different Methods of Integrating Single Sign-On

Implementing a Central Filter

The phrase Man-in-the-middle tends to engender a certain feeling if ill intent or malevolence – as noted above, it is typically used in reference to an individual who intercepts information in transit for use to gain access to a network or database. While this typical assumption is more or less accurate, it is by no means the sole purpose for a man-in-the-middle.

By way of a proxy server or similar intervention - much like black hat and white hat are two sides of the same coin in hacking - the functions of a man-in-the-middle can be used as a central filter to help improve the security around your sensitive data as well.

Three instances come to mind: redacting information, regulating file downloads and blocking access to potentially malicious websites.

Redacting Information

Characteristically, people think of classified government information when the term redacted is mentioned. We think of segments of text that are blacked out and rendered indecipherable when looked at. Redacting protects information that cannot be viewed by the eyes of anyone without authorized clearance.

In terms of data security, redacting is used in much the same way. By integrating the central user repository within your environment to a secure portal, you can use the same notion of redacting that the government uses for classified documents to regulate what information is seen by individual users or groups. Redacting is, at the most basic level, a form of blocking information, and it comes in two forms: blocking an entire page or specific data on said page.

Essentially, an administrator can customize web pages behind a secure portal to display or hide specific sections based on the organizational unit of his or her choice. Redacting through a central filter can only be done on web-based pages, as opposed to downloadable content. Administrators view the web page through the customization panel and select which sections of the page are to be blocked off for which organizational unit. The depth of this configuration will depend exclusively on the person doing the configuration – making sure that the correct information is redacted and no error in judgment occurs, the likes of which may be seen if software is used to determine what information is redacted.

The most secure method of access control is to provide users with the exact amount of access that they need-no more and no less.

By implementing a central filter by way of a proxy server, administrators have full discretion over which information is blocked for whomever may view the web page. The most secure method of access control is to provide users with the exact amount of access that he or she needs – no more and no less.

Regulating File Downloads

While redacting information is a useful tool for resource management, the ability to extend access control to specific files or resource downloads is another beast entirely. A major concern for many industries is the loss of data as it makes its way from a secure network, onto a mobile (here meaning movable) machine and into potentially unsecure territory. By enabling the control and regulation of resource downloads, you can essentially mitigate this risk.

Another benefit of using a central filter is the use of Contextual Authentication (AKA Risk-Based Authentication). The central filter - here being the identity provider - can associate various aspects of authentication attempts to individual risk scores. Then, using these scores to calculate a relative risk threshold, access to resources can either be granted or denied.

Contextual Authentication takes various attributes of a login attempt – geolocation, network type, time of day, etc. – and compiles a configurable risk assessment to determine the necessity and validity of a login. This can be used to regulate external, remote access to the network, as well as resource control for file downloads.

Ideally, the benevolent solution acting as a central filter will compare the associated risk score to the resources in question to determine whether or not the file can be downloaded. Perhaps a user or group has every right to download a payment report during normal business hours on their local machine, but is not permitted to access this data from another machine, or during off-business hours. Given the full customization of this process, a single failed check on the status of the request can prevent the download from commencing – protecting sensitive data from the first point of access.

Control Website Access

The more traditional role for a proxy server is controlling access from an organization's network out to the internet. Forward proxies would typically be used to prevent end-users from accessing illicit content. However, this same approach can be used to dynamically block access to websites that are "known" to be malicious or those that are hosted in other countries. This can help ensure end-users that unwittingly click on URLs in phishing emails are not fully phished because access to the malicious website in question is blocked by the network itself.

Multifactor Authentication

The term 'Multifactor Authentication' is often thrown around without due explanation. Typical assumptions tend to revolve around Multifactor as an obtrusive, expensive add-on to already obnoxious login protocols. While this may have been the case when Multifactor first joined the scene, it remains one of the most significant methods for securing data in this password-driven world.

Multifactor Authentication (often referred to indirectly as Two-Factor Authentication) is the use of two or more independent credentials; the typical mantra is that an individual must login with something s/he knows (username and password), something s/he has (a hard or soft token and OTP) and/or something that s/he is (biometrics). While oftentimes over exaggerated to the point of confusion, Multifactor is commonly used in many situations today.

Typical examples of Multifactor include:

- Chip and Pin enabled credit cards
- Answering security questions before gaining access to your banking information
- Entering a One-Time Password before being able to login to a phone or computer application

Where sensitive data security is concerned, the proper implementation of Multifactor Authentication can mean the difference between a huge financial loss due to a corporate data breach, and a minor inconvenience when a password gets stolen.

Modern Multifactor Authentication has transcended leaps and bounds beyond typical hard-tokens and bulky, expensive biometric scanners. Solutions now have the capability to use mobile phones, cheap USB tokens, website cookies, or any combination thereof to provide Multifactor Authentication – all in an effort to increase security without hampering convenience and usability.

After all, you wouldn't trust your valuables behind a door that just anyone can open – Multifactor Authentication makes certain that only the right person has the key to any sensitive information.

Strong Password Policies

It is a stalwart truth of the modern digital age that the password is still a significant aspect of authentication and security. Regardless of the use of biometrics, tokens or other roundabout methods of logging into various services, the base requirement is a password. While some might call for the death of the password and decry its various weaknesses, the fact remains that the password is – for the time being at least – here to stay. With that in mind, it is important to protect this front line of defense against any attack or compromise to better secure any data that may lie behind it.

Password policies vary widely from organization to organization. Security requirements, auditing and compliance necessities – these things are just the tip of the iceberg of conditions that can affect the layout of a password policy. Unfortunately, while a more in-depth and complex policy can dramatically increase security, it can be difficult to find a method of enforcing said policy without alienating end-users.

Fortunately, enforcing password policies is as simple as implementing a user-friendly solution to handle the four most basic aspects of a strong password policy:

- Password History
- Password Age
- Password Length
- Password Complexity

Password History

Password history refers to the ability for a solution to recall a specific number of recent passwords on a per-user basis. While many individuals understand the need to reset passwords on a basic level, the importance of password history configuration can often be left by the wayside.

By enforcing password history requirements, an organization will prevent users from rotating through multiple common, easy to crack passwords. This serves as an introduction to security aspects, and in conjunction with other configuration methods for password policies, will serve to strengthen the overall front door to sensitive data.

Password Age

The age of a password is also important to consider when creating a strong password policy that needs to be enforced. There are two primary settings for password age: minimum and maximum. Typically, most people think of maximum password age as the most important requirement, but the minimum age is also paramount in creating a more secure environment. Minimum password age represents how long a user must have a password before it can be changed. Proper configuration of this setting will prevent users from creating and resetting passwords to clear out the password history to enable a simple, potentially less secure password to be used.

Minimum password age requirements, combined with password history settings, can serve to further prevent users from making use of common passwords, or reusing older passwords. While an older password may be more convenient for an end-user, it also may have been compromised. By reducing the likelihood of old password usage, your environment is adding an extra layer of protection against possibly compromised credentials.

Maximum password age is the parameter that denotes the rate at which a password must be changed. Standard practice is to use a lower interval in environments where security is paramount. Strong parameters for maximum password were traditionally shorter intervals of 30 or 60 days, but guidance from standards bodies such as NIST have more recently eschewed these shorter periods. The emphasis now is on creating stronger "passphrases" that no longer expire periodically at all[viii]. Instead, the recommendation is that users should only be forced to change their password if there is evidence it was compromised. This could be its appearance in a list of exposed passwords/password hashes or if fraudulent activity is detected on the account.

Password Length

Another staple for password requirements is password length variations. Every organization has its own view of what the optimal password length actually is, but one realization always remains the same: password length has a hefty impact on password strength. Setting the appropriate password length, along with more rigorous password complexity settings, decreases the likelihood of a password succumbing to typical attacks, which in turn increases the strength of the security surrounding any sensitive data.

Password Complexity

Length is not the only definitive characteristic in password strength. The complexity of the password protecting sensitive data is of key importance in providing the strongest front line possible. While password length refers solely to the number of characters in the password, complexity encompasses multiple additional requirements including:

- Letter Case
- Alphanumeric Characters
- Character Set
- Allowable Special Characters
- Dictionary Blacklisting

Each additional complexity requirement exponentially increases the strength of the password that is protecting sensitive data. If all else fails, increasing the complexity of the password to a manageable level within the password policy will provide a huge boon to your security and work towards making the success of an attack much less likely.

As alluded to earlier, there are now stronger recommendations to emphasize the use of "passPHRASES" instead of "passWORDS". It is easier for users to remember multiple words rather than character substitution (e.g. "1" for "i", "O" for "0") which is commonly attempted by hackers. The use of phrases also results in longer passwords which is the most important determinant of how difficult it is to crack a password.

Enforcing Password Policies

It is important to keep in mind that securing sensitive data relies heavily on the success of any initial security measures. Creating a strong password policy is a fantastic way to drastically increase security on paper – but user adoption and adherence is key towards actually establishing that increase in security. Adherence to a stringent password policy may require some trial and error on behalf of end-users, and implementing a self-service solution is an additional method of balancing security and usability.

Self-Service Password Reset (SSPR)

End-users are always working to meet one deadline or another – and oftentimes the stress of the job can lead to forgetting a password, or simply mistyping it one too many times. Unbelievably, many organizations still require that account lockouts and password resets be taken care of through the help desk – drastically increasing end-user frustration, and the likelihood that users will attempt to find workarounds to avoid adhering to what can be seen as an arduous requirement.

Implementing an SSPR solution puts the power of convenience and security back in the hands of the end-user. Additionally, an SSPR solution provides users with the ability to easily adhere to more stringent password policies without feeling any extra stress when a password simply won't work when they need it too.

Increased security measures are only effective if the users find them tolerable and easy to manage. Proper configuration of password policy settings alongside appropriate user-experience considerations goes leaps and bounds ahead for securing your sensitive data in the front lines where many attacks take place. SSPR helps toe the line between security and convenience and keeps your end-users happy and productive throughout the day.

BONUS—Never Underestimate the Human Factor

An important thing to understand about data breaches and security is that eventually, if you follow the trail far enough, you will always find a person at the beginning - A flesh and blood, intelligent human being who decided to play with the black hat for once in his or her life. It is an unfortunate truth that not every end-user is trustworthy. Creating a strong security policy is a magnificent first step in protecting sensitive data, but it can all be undone if there are no safeties to address the human factor in security.

The name Snowden is known practically worldwide now, and is virtually synonymous with data security and the leaking of sensitive data. One thing that people often forget – or simply do not realize – is that the incidents surrounding Snowden were because of an inside job. Information was copied to a drive and released to external sources, placing wildly sensitive data into the eyes of the public. While we offer no judgment either for or against here, the point remains: end-users can be a potential threat as well.

The importance of additional tools to combat this threat is essential when attempting to secure sensitive data. Making use of secure portal integration, Single Sign-On, Self-Service and Multifactor Authentication is a grand step, but even these can be overcome if not watched carefully.

Accurate, consistent reporting and logging are key requirements to address the human factor in sensitive data security. Implementing a rigid reporting solution will mitigate risk from undocumented changes to the environment or the network, and will work in tandem with proper Contextual Authentication methods to guarantee that data is only being accessed by the correct user.

Never forget: the biggest threat to your security lies within your own environment.

The biggest threat to your security lies within your own environment.

Conclusion

While some may look to data breaches and cyber attacks as a statistically unlikely event, the facts speak for themselves. By May of 2015, the Ponemon Institute and IBM reported that the average cost of a data breach had risen to a somewhat staggering $3.79 Million, with over 350 companies being victims in 11 different countries[IX]. The reality is that anyone can become a victim of a cyber attack – and sensitive data security has never been more important.

Improving security doesn't have to be a nightmare of an endeavor, however. By implementing the best practices discussed throughout this paper and taking a hard look at your approach to security as well as your end-users, you can significantly improve your defense against cyber attacks and suspected data breaches.

Security is a constantly changing field – and it takes vigilance and dedication to keep it under your control. Where sensitive data is concerned, cutting corners and ignoring facts will only increase the likelihood of a data breach in this primarily digital world. Finding a strong balance between security and usability will provide you with the foundation that you need to keep the beast under control.

The future is here – we don't have to make sacrifices to secure our sensitive data. Follow these best practices, and find the solution that works best with you. The attackers won't stop trying to steal your data; you shouldn't stop working towards keeping them out.

Questions?

Contact our Authentication Experts

Phone: +1 (603) 547-1200

Email: sales@portalguard.com

Resources

[i] http://simonsingh.net/books/the-code-book/

[ii] http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/

[iii] http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/#72c917ae7c7b

[iv] http://www.forbes.com/sites/davelewis/2014/12/17/sony-pictures-how-the-criminal-hackers-won/#510b70a540f6

[v] http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

[vi] https://www.idtheftcenter.org/data-breaches/

[vii] https://www.kb.cert.org/vuls/id/475445

[viii] https://pages.nist.gov/800-63-FAQ/#q-b5

[ix] https://www-03.ibm.com/press/us/en/pressrelease/47022.wss