White Paper by Expert Insights

Identity And Access Management For Financial Services

A Comprehensive Guide

Published
March 2022

Expert Insights

Sponsored by
HID Global

01 Executive Summary

Introduction

Financial services is one of the most frequently targeted industries when it comes to cyberattacks. And it might come as no surprise that money is a key motivator.

In fact, a massive 92% of all attacks are estimated to be financially motivated—with espionage, grudges, fun, and ideology accounting for the remaining 8%.[1]

But while financial services organizations are an attractive target for cyber-criminals looking for a large profit and to wreak havoc on some of the world's trusted and most profitable businesses, cyberattacks aren't an unavoidable threat as long as you have the right protection in place.

Throughout this guide, we'll take you through six identity and access management best practices for businesses in the financial services industry. We'll cover some of the key challenges facing financial institutions in today's ever-evolving digital climate, as well as how you can best secure access to your accounts to minimize your risk of attack.

"Financial services is one of the most frequently targeted industries when it comes to cyberattacks. And it might come as no surprise that money is a key motivator."

Key Takeaways

1. Financial services is an industry that's frequently targeted by cybercriminals looking to make a profit from or create damaging consequences for trusted businesses. And with the prevalence of remote working and with the rise in social engineering, business email compromise (BEC), and insider attacks, a robust identity and access management protocol is now more important than ever.

2. User passwords are known to be notoriously weak, while credential compromise is only becoming a more prevalent challenge for organizations in financial services. But businesses should seek ways of authenticating that strengthen security while minimizing friction to the user journey.

3. Financial services organizations should follow best practices to secure their businesses against targeted attacks. Recommended advice includes implementing multi-factor authentication and single sign-on, ensuring strong access to digital and physical corporate resources, using biometric technologies, implementing a robust security policy, and following Gartner's CARE framework for access management.

02

Why Is Identity And Access Management Important?

The rush to digitize during the Covid-19 pandemic left businesses globally vulnerable to a whole new range of threats—and the financial services industry has seen no exception. At the beginning of the pandemic the industry saw a 238% increase in cyberattacks, with ransomware increasing by 9 times.[2] And the hits have only kept on coming.

Here are some of the other challenges facing the industry today.

Sophisticated Cyberattacks Are Increasing

Attacks most prevalent in the financial services industry include social engineering, ransomware, BEC, and distributed denial of service (DDoS). And all of these are only growing more advanced with the development of new methods and technologies.

In fact, cybercriminals are known to pool their resources and information to execute more targeted attacks as well as invest profits from successful attacks into developing even more sophisticated and damaging technologies.

Crime groups are even beginning to function more akin to established businesses, with pre-determined roles and helplines for ransomware victims, according to a cybercrime report by the Telegraph.[3]

Credential Compromise Is Becoming More Prevalent

Passwords are a long-standing challenge for businesses—with 50% of IT professionals regularly reusing the same passwords across work accounts.[4] While 24% of Americans also use weak passwords like “Password” and “123456”.[5]

As well as passwords being notoriously insecure, credentials are compromised in 32% of all attacks against the financial services industry.[6] So, if your users’ accounts are solely password protected and your users are using weak passwords, then a breach isn’t just likely, but inevitable.

But making passwords more secure by making them more complex means only adding friction to what’s already an impossible expectation on users. Which is why an improved way to strengthen user credentials is needed.

The Challenges Of A Multi-Channel Environment

The prevalence of remote working has introduced its own challenges for the financial services industry—and for some businesses, remote working is part of a permanent culture shift that's here to stay.

Many organizations have struggled with the complexity that comes with securing identity and access across evolving multi-channel environments. In fact, 42% of financial services organizations agreed that the need to work remotely due to the pandemic negatively impacted their security posture.[7]

Security also comes under the responsibility of your users—you expect them to act safely and securely, so they need the technologies in place to support them with that.

The Need To Adhere To Compliance Standards

Responsible for safeguarding sensitive data and finances, adhering to compliance regulations and standards is crucial for businesses in the financial services industry. And many regulations include secure identity and access management practices in their regulations.

A regulation for financial services that mandates secure identity management is Sarbanes-Oxley (SOX), which requires organizations to have robust internal controls, policies, and procedures in place to prevent fraud and protect data.[8] Another example is the Gramm-Leach-Bliley Act (GLBA), which requires businesses to actively take measures to prevent unauthorized access to information and sensitive data.[9]

Personal data is also compromised in 83% of attacks against financial services, while bank data accounts for 33%.[10] Failing to comply with data protection standards such as the General Data Protection Regulation (GDPR)—if you're based in the EU—can land you a fine of up to €20 million or 4% of your annual revenue, depending on severity.[11]

A Zero Trust Approach Is Needed

With the shift to remote working and cloud environments, as well as the prevalence of BEC and insider attacks, it's dangerous to assume that all users either already on or entering your network are trustworthy.

Zero Trust is a philosophy centered around one simple concept: trust nothing and no one with access to your accounts, systems, and networks without continuous identity verification.

A Zero Trust architecture is integral when it comes to identity and access management, as it advocates for continuous user authentication and monitoring using multiple factors, as well as only granting users access to the accounts and systems that they need for their roles.

And Zero Trust is only becoming more vital for organizations globally. As an example, following the disastrous consequences of the Colonial Pipeline attack in the US in May 2021, President Joe Biden issued an executive order that required for Zero Trust to be implemented across all government departments as part of a plan to improve security practices.[12] This just goes to show how integral a Zero Trust architecture is in an evolving threat landscape.

"Zero Trust is a philosophy centered around one simple concept: trust nothing and no one with access to your accounts, systems, and networks without continuous identity verification."

03 Best Practices

In the following section, we'll break down six best practices for securing your identity and access management processes.

1. Implement Multi-Factor Authentication

Multi-factor authentication (MFA) is a login method whereby users must use two or more factors to authenticate their identities. And this has been proven to prevent an astonishing 99.9% of attacks.[13]

Factors that can be used to authenticate come in three broad categories:

1. Using something they know: This is known as knowledge-based authentication, and includes the use of passwords, PINs, and answers to secret questions.

2. Using something they have: This is possession-based authentication, and includes authenticator apps, smart cards, and one-time passcodes.

3. Using something they are: This is inherence-based authentication, and includes biometric technologies such as fingerprint scanners, facial recognition, and behavioral measurements.

With MFA in place, users can be prompted to use their password alongside both a fingerprint scan and a notification to their authenticator app, for example.

But not all factors are made equal, and they can vary in terms of security and ease of use. So, it's vital that you choose factors based on the level of security you need as well as considering the use cases across your organization.

"Multi-factor authentication (MFA) is a login method whereby users must use two or more factors to authenticate their identities.."

The Benefits Of Securing Accounts With Multi-Factor Authentication

The key benefits of implementing MFA across your user base include:

- Reducing the risk of a breach: If a user's credentials are compromised, a cybercriminal still wouldn't be able to access their account without passing the second or third factor of authentication.
- User convenience: MFA is easy to use, offers many modes of authentication, and can strengthen security while being relatively frictionless for users.
- Compliance with industry standards: Implementing MFA helps you comply with industry standards such as SOX, PCI DSS, and NIST.
- Ease of implementation: MFA can be quick to deploy, integrates well with existing systems, and requires little to no end-user training.
- Adaptive MFA: Many enterprise MFA solutions offer adaptive authentication, which means IT security admins can determine the level of security required based on the context of each login attempt.

2. Implement Single Sign-On

Single sign-on (SSO) is a solution that enables users to log into all connected accounts using just one set of credentials.

This is because SSO comes under the federated identity management (FIM) umbrella.[14] This is essentially a partnership between providers where, if a user is authenticated by one partner, they're automatically granted access by their trusted partners.

When a user logs into an SSO platform, this creates an authentication token for the user. The system then enables them to automatically log into any connected application that they open by sending the SSO token to the provider to prove their verified status, negating the need to enter a new set of credentials each time they use a different application.

It might sound risky to secure access to multiple accounts using just one set of credentials—and, if done improperly, it can be. Which is why we recommend securing SSO accounts with strong MFA and using a trusted identity provider.

The Benefits Of Logging In Using Single Sign-On

- Improved user experience: SSO provides a user-friendly and frictionless experience by reducing password fatigue and eliminating the requirement to log in using new credentials each time a user switches application.
- Increased security: Logging in via SSO reduces the attack surface significantly and helps to address poor password practices.
- Standards-based login: SSO takes a standards-based approach to authentication and authorization—using protocols like Security Association Markup Language (SAML), which exchanges data between vendors and applications that details user identity for authentication, and entitlement and attributes for authorization.[15]
- Greater controls for security teams: Security teams can leverage greater visibility across accounts, more granular centralized access controls and policies, and simplified reporting and auditing processes.
- Move to passwordless authentication: SSO can be used to simulate a passwordless experience and is considered the first step towards a passwordless architecture.

3. Ensure Strong Physical Identity And Access Management

As many employees return to the office either full-time or in a hybrid way, and with insider threats being a prevalent challenge for financial services, strong physical access security should be implemented to complement digital identity and access management technologies.

Physical identity and access management (PIAM) solutions manage identity and access policies and procedures for physical assets.[16] PIAM sits above multiple systems and holistically manages user identities, permissions, credentials, and physical access policies from one central area.

This means not only allowing users access to facilities based on a valid credential, but also based on contextual factors, access policies, and more.

Identity can be proven in a number of ways. A common way is by implementing a physical card which can be used as visual identification and physical access at barriers. These can be used across your workforce as well as to authenticate third parties and visitors.

To further improve both security and user convenience, we also recommend the convergence of logical and physical access controls. This is a unified approach that enables users to leverage one credential to access a range of digital and physical assets. This also means that permissions can be easily granted or revoked across all assets, depending on the level of access required by the employee.

“Physical identity and access management (PIAM) solutions manage identity and access policies and procedures for physical assets. PIAM sits above multiple systems and holistically manages user identities, permissions, credentials, and physical access policies from one central area.”

The Benefits Of Strong Physical Identity And Access Management

- Reduced security risk: With admin-configured policies and granular permissions, only authorized individuals are allowed access to sensitive areas and information, protecting against insider threats.
- Frictionless authentication for users: A robust PIAM solution enhances security while providing a seamless user experience.
- Real-time monitoring and updates: PIAM solutions continuously monitor identity and access activity—including which users accessed which facilities, what times, and more. Using machine learning technologies, you can also identify suspicious behaviors in real-time—where users are attempting to access facilities that they don't have the right permissions for.
- Proving regulatory compliance: PIAM solutions are designed specifically to prove compliance with financial services regulations —SOX, for example—and provide reliable auditing trails that show where access was granted or revoked for specific employees.
- Reducing manual efforts: Automating identity lifecycle workflows and access policies reduces the need for manual physical security checks and authorization.
- Implementing Zero Trust: PIAM supports a Zero Trust architecture by providing access from the ground up, and only providing users access to areas that are needed for their specific roles.

4. Use Biometric Security Controls

Earlier, we mentioned that not all factors are made equal. And that rings especially true when it comes to inherence-based factors like biometric authentication.

Biometric technology works by measuring users' unique characteristics to authenticate their identity. These characteristics can either be physical (fingerprints, face recognition, iris scanning) or behavioral (the way a user types, walks, or speaks).

This type of authentication is quickly gaining traction in the financial services industry—with the market expected to grow 12.8% by 2026—and is generally considered by experts to be the most secure way of authenticating user identity.[17]

This is because it's based on a probabilistic system, which analyzes a number of contextual factors to calculate the probability that the user attempting to log in is authorized to do so. While, knowledge-based methods of authentication, like passwords, will let a user into an account based on them simply knowing the right answer.

For maximum account security, we recommend pairing biometric technologies with multiple other factors, to establish a comprehensive MFA login system.

The Benefits Of Securing Accounts Using Biometric Authentication

The benefits of using biometric technologies to verify users' identity include:

- Security: Biometric traits are non-transferrable and difficult to spoof. And, if stored securely—for example, locally on-device, so that data never leaves users' devices—can be incredibly secure.
- Improved user experience: Biometrics are easy to use and can facilitate a passwordless login, which means a frictionless user experience and eliminating the challenges that come with passwords. And, after all, a complex password can slip your mind, but your fingerprint isn't so easy to forget.
- Flexibility and adaptability: Not only are there a wide range of biometric characteristics for users to choose from based on their use cases, devices, and abilities, but they can also be used to secure both digital accounts and physical office environments.

"Biometric technology works by measuring users' unique characteristics to authenticate their identity."

5. Implement Strong Security Policies

A security policy is a living document that defines a set of rules and procedures to be followed by everyone across your organization. This includes information on your identity and access management procedures and permissions, such as MFA requirements and granular role-based access policies.

Your policy is vital for protecting the confidentiality, integrity, and availability (CIA) of data, and is often a requirement to comply with many industry standards. For example, the ISO 27001 standard requires you to establish an information security policy to achieve certification.[18]

Your policy should not only detail access requirements for your organization as a whole, but also departments, teams, and individual users. Within the policy, you should identify all of your assets and potential threats, to put in place measures to protect those assets. A strong identity and access management tool can help you not only implement but also enforce your policy across your organization.

You should also regularly revise and update the policy, as well as ensure all employees and third parties are familiar with its contents. The policy should also be readily available for your customers to review at any time.

We recommend that you work to develop the right policy for your organization's specific set of requirements. Various frameworks—including NIST and ISO—offer guidance around creating and maintaining security policies.[19,20]

> "A security policy is a living document that defines a set of rules and procedures to be followed by everyone across your organization."

The Benefits Of A Strong Security Policy

The benefits of implementing a robust security policy include:

- Securing valuable data and assets: Security policies are designed to keep sensitive data and assets safe and apply to physical premises as well as digital access.
- Ensuring the right controls are in place: Having your procedures written within your policy helps you to ensure you're taking the right actions to protect your organization against any looming threats.
- Communicating rules and procedures: Your policy communicates to your employees and third parties what your IAM practices are, what's expected of them, and how they should act.
- Adhering to standards and regulations: Your policy outlines the responsibilities and actions users should follow to adhere to regulatory compliance, as well as consequences of non-compliance. A policy is also a way for you to prove compliance during audits and might be a requirement to be eligible for coverage by cybersecurity insurance, too.
- Implementing Zero Trust: Security policies are fundamental to a Zero Trust framework, as within them you can implement and configure granular access policies for users and teams.

6. Follow Gartner's CARE Framework

Finally, the impact and overall success of your identity and access management processes should be easily measurable via a set of defined metrics. Which is why our final recommendation is to follow Gartner's CARE framework for security controls.[21]

In 2019, following a proposal to issue record fines to Marriott International Inc. as a result of a GDPR breach, UK Information Commissioner Elizabeth Denham said that a key focus was: "whether or not there was adequate, reasonable, consistent, effective data security to protect people's data."[22]

Gartner developed the CARE standard as a method of measuring and developing the effectiveness of security controls and processes with regard to these considerations. Instead of simply checking whether an organization has invested in a particular tool or follows a certain procedure, CARE is outcome-based and looks at the outcomes of using those technologies.

"Gartner developed the CARE standard as a method of measuring and developing the effectiveness of security controls and processes with regard to these considerations."

To measure the success of your security program, CARE looks at the outcomes of whether a program is consistent, adequate, reasonable, and effective (CARE):

Consistent: Controls should be stable and work consistently in the same way over time across your entire organization.

Adequate: Controls should adequately reflect and complement your specific business needs, priorities, and expectations.

Reasonable: Controls should be appropriate, fair, and moderate, and cause minimal friction for users and your business.

Effective: Controls should achieve your desired outcomes.

Gartner recommends tracking 20–30 CARE metrics to help you understand and analyze your organization's overall security posture.

The Benefits Of Following Gartner's Care Standard

The benefits of following the CARE framework for security controls include:

- Improved security: CARE helps organizations to put in place identity and access management processes that are high-quality, reliable, and actually work. This helps improve security not just at the time of implementation, but over time too.

- Improved user experience: The framework suggests reasonable login controls, that are appropriate for each use case and cause minimal friction and frustration for users during the login process.

- Assessing outcomes: Gartner designed CARE to help implement and continuously measure program outcomes. You can use CARE to ensure your program is continuously developing and evolving, based on whether your desired outcomes are being met or not.

- Meeting regulatory compliance: The framework is designed to help you more easily comply with industry standards and regulations.

04 About HID Global Solutions

As an experienced partner in banking and financial services—as well as many other high-security industries—HID Global's robust solutions focus on protecting users and sensitive data both conveniently and securely. Its advanced, easy-to-use solutions range from people-centric MFA and PIAM to highly secure smart cards for converged physical and logical access and security keys.

HID Digital Persona

HID DigitalPersona DigitalPersona is a robust MFA solution that goes beyond the typical modes of authentication to provide flexible and frictionless—yet secure—Windows logon and VPN access for users. It's ideal for organizations within healthcare, manufacturing, retail, call centers and others where users need rapid access to shared workstations during the course of their working day.

DigitalPersona combines the traditional factors of what you know, have, and are, with contextual risk factors of time and location. The latter covers where you are (IP addresses), and when you act (login timeframes), allowing organizations to precisely match their risk exposure to the optimal security posture for their needs. By adding additional features such as SSO, password manager, or Access Management API, you can secure all applications across your entire user base using the factors that are best suited for each specific user, device, app, or network.

In addition to supporting the market's broadest array of authentication methods, DigitalPersona works with various form factors ranging from smart cards and building access cards, FIDO- and PKI-enabled security keys, mobile devices including OTP, push notifications and Bluetooth, to biometrics including fingerprint and face.

Crescendo Smart Cards

Crescendo smart cards are ideal for ensuring secure and seamless authentication for employees organization wide. These smart cards act as a converged corporate badge, securing access to physical premises and facilities as well as applications, networks, and systems, using just one convenient credential.

Crescendo smart cards also help implement a Zero Trust foundation by ensuring employees are provided access only to the facilities, assets, and information that's needed for their roles.

The Crescendo smart card range is fast to deploy, Microsoft compatible, and designed to comply with regulatory compliance—the range supports multiple security standards such as FIDO2, OATH, and PKI, while also being Federal Information Processing Standards (FIPS) 140-2 Level 2 certified.[23]

Crescendo Security Keys

HID Global's Crescendo Security Keys with FIDO2, PKI/PIV, and OATH capabilities are designed to offer users fast, easy-to-use, and secure passwordless authentication to corporate networks, applications and data.

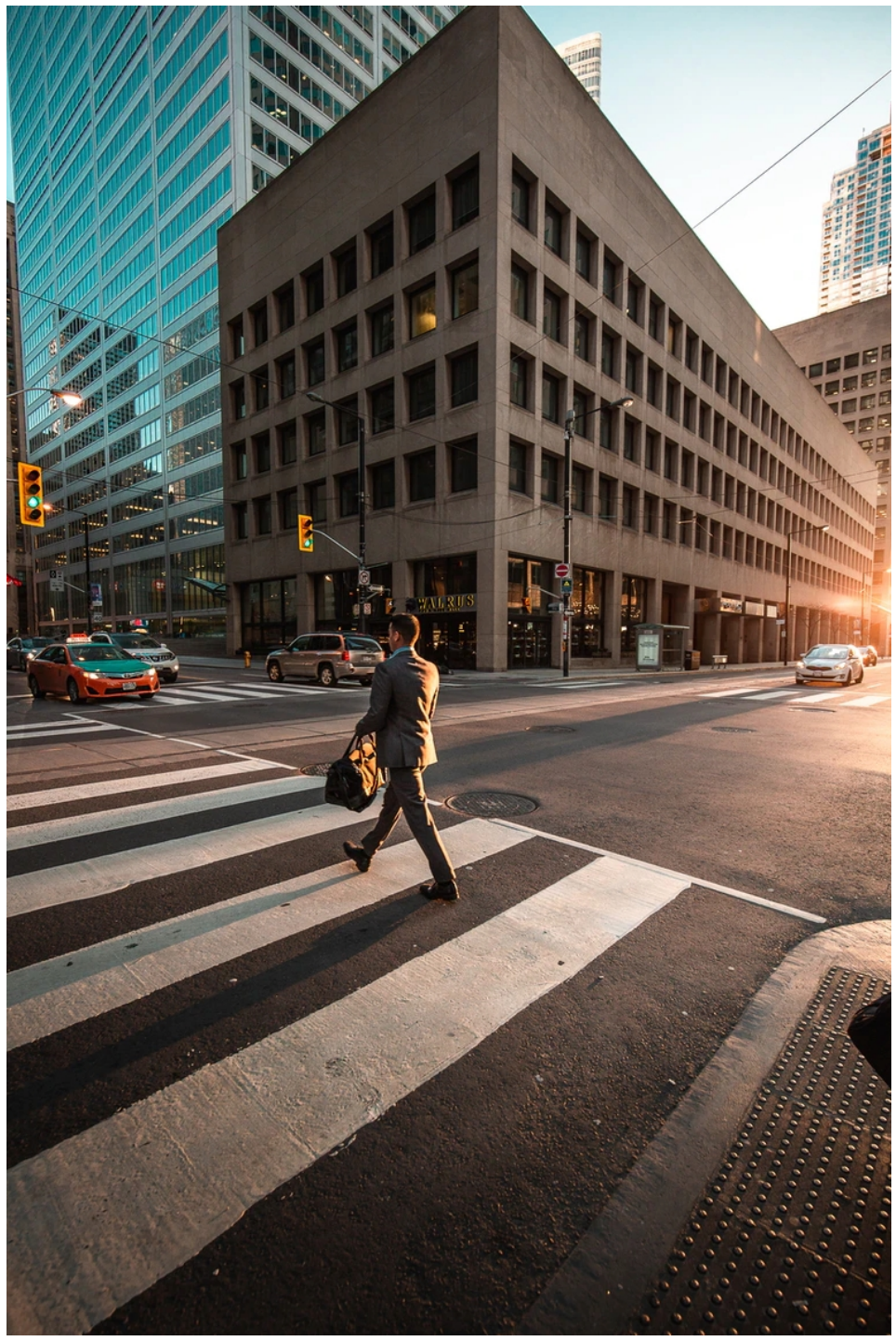
The Crescendo keys utilize near field communications (NFC) and USB-A and USB-C while offering a convenient form factor that complements laptops and tablets without the need for additional reader hardware.

05 Summary

A truly secure financial services organization means secure access to your accounts, systems, and networks. Just one small crack in your identity and access management solution can be wide enough for a significant threat to slip through.

But by following our best practices, you can not only add those additional layers of security to your login process but also simultaneously reduce friction for users and provide them with easier, faster, and more accessible methods of logging into their accounts.

To help you achieve a more secure and frictionless login, we recommend HID Global's DigitalPersona for robust, adaptable MFA capabilities, as well as the Crescendo smart card to secure access to your facilities and technologies.



06 Sponsor Of This White Paper

HID Global is a market-leading provider of identity security solutions for physical and logical (digital) asset authentication. An independent brand of Swedish door and access control provider ASSA ABLOY, HID Global manufactures and sells a variety of physical and logical access control solutions, as well as secure issuance products to accompany those solutions. These include smart cards, card readers, card printers and encoders, cloud services, IoT identification technologies, and identity and access management software.

From their headquarters in Texas and worldwide international offices, HID Global work with organizations in over 100 countries across a number of verticals, including government, education, finance and aviation, helping them to implement trusted physical and virtual environments founded on

www.hidglobal.com
Twitter: @HIDGlobal
LinkedIn: @hidglobal
customerservice@hidglobal.com
Tel: 800-872-5359

07 About Expert Insights

About Expert Insights

Expert Insights is a global, independent resource for organizations around the world to research and compare business IT solutions and services. Our number one goal is to help businesses research and find the right solutions to solve their security problems. To help organizations achieve this, our independent editorial team have created buyers' guides, resources, vendor comparisons and interviewed industry leaders, so that our users can research and compare solutions on one technology focused platform.

08 References

References

1. https://www.verizon.com/business/resources/reports/dbir/

2. https://blog.bio-key.com/three-major-security-challenges-finance-avoid

3. https://www.telegraph.co.uk/business/ready-and-enabled/cybersecurity-for-businesses/

4. https://www.comparitech.com/blog/information-security/password-statistics/

5. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

6. https://www.verizon.com/business/resources/reports/dbir/

7. https://www.baesystems.com/en/cybersecurity/article/covid-cyber-crime-74-per-cent-of-financial-institutions-experience-significant-spike-in-threats-linked-to-covid-19

8. https://identitymanagementinstitute.org/sarbanes-oxley-access-management-requirements/

9. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

10. https://www.verizon.com/business/resources/reports/dbir/

11. https://gdpr-info.eu/issues/fines-penalties/

12. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

13. https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

14. https://www.techtarget.com/searchsecurity/definition/federated-identity-management

15. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

16. https://blog.hidglobal.com/2021/11/what-piam-and-why-do-i-need-it-if-i-have-pacs

17. https://www.helpnetsecurity.com/2021/06/11/biometrics-for-banking-market/

18. https://www.iso.org/standard/54534.html

19. https://www.nist.gov/cyberframework

20. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

21. https://www.gartner.com/en/articles/4-metrics-that-prove-your-cybersecurity-program-works

22. https://www.wsj.com/articles/u-k-regulator-on-why-it-is-pursuing-record-fines-against-ba-marriott-11562751006

23. https://www.encryptionconsulting.com/education-center/what-is-fips/