Cybersecurity & Payments:
For Banking & Finance

kiuwan
An Idera, Inc. Company

INDEX

Overview

Financial service providers, such as banks and financial institutions, are entrusted with sensitive data, including social security numbers, financial details, addresses, and so much more. Since this data is highly attractive to cybercriminals, such organizations are always at a security risk.

Advances in technology have led to the development of banking apps and similar channels. However, the technology is also susceptible to attack by nefarious intruders and hackers since application security is a big concern.

With time and continuing advances, certain vulnerabilities have emerged of which it is imperative that the finance sector be aware. In this guide, we'll take a look at finance and banking security and discuss aspects pertaining to application security and payments cybersecurity.

Why Is Cybersecurity Important in Financial Institutions and Banks?

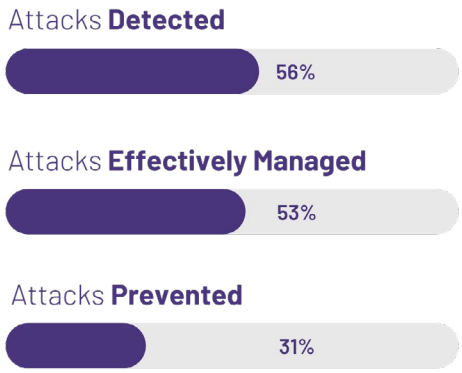
Cybersecurity is a huge concern in financial institutions and banks these days as customers entrust these institutions with their personal and sensitive information in order to make online transactions.

Unfortunate cyberattacks have led to data breaches, identity thefts, and similar hacks that have resulted in huge monetary losses for financial institutions.

Security leaders at Mastercard reportedly told the New York Times that the credit card company faces nearly **460,000 intrusion attempts in a day**. In fact, the company showed the news organization monitors that tracked **267,322 attempts in just 24 hours**.

Mastercard is not the only company facing this particular issue. According to a 2017 survey by Ocum, **40% of banks get 160,000 erroneous**, irrelevant, or duplicate cybersecurity alerts every day.

Unfortunately, the financial industry is more effective at detecting attacks than preventing them in the first place. According to a Ponemon Institute survey of 400 security professionals, the financial service industry detects **56%** of the attacks, effectively manages **53%**, and only prevents **31%**.



Considering these statistics, it is clear that the financial service industry must prevent the attacks in the first place since customers entrust them with sensitive information. Here are some reasons application security and payments cybersecurity are important in banks and companies providing financial services.

Prevents Financial Losses

When a bank experiences data breaches, it suffers significant financial losses. On the one hand, its customers lose their money. On the other hand, customer trust in the bank is tarnished and the bank's reputation negatively impacted

JP Morgan Chase reports spending $600 million on cybersecurity. The amount may sound quite hefty to some, but when you take the expected risk of poor cybersecurity practices into account, this is a much lower price to pay.

According to a study by Accenture, *"The average annualized cost of cybercrime for financial services companies globally has increased to US $18.5 million — the highest of all industries included in the study and more than 40 percent higher than the average cost of US $13 million per firm across all industries."*

Banks must have a cybersecurity plan in place in order to effectively counter cybercrime.

Banks must also offer online banking security services to prevent their customers from losing money through data breaches, which can happen even if the bank has a good cybersecurity system in place.

Protects Customer Data

When a customer opens an account in a bank or logs in to the bank's app, they share a lot of sensitive information, such as their social security number.

In the case of a breach, this information could fall into the wrong hands, and fraudsters could then use it to open new accounts or steal the customer's identity.

Banks that offer their employees training in cybersecurity provide a layer of defense against fraudsters who might try to access this information from within the bank itself.

In addition to offering online security training for employees, banks can also protect their customers by ensuring that all customer data is encrypted when it leaves the device.

However, it is important to note that there are other threats to look out for as well. In addition to threats from outside of a bank, banks must also protect against threats from within their own organization.

Employees could mistakenly or deliberately release sensitive information without proper security training.

For example, a nontechnical employee would not know how to encrypt customer information on a flash drive. An experienced hacker might break into the system and steal that same information from within the bank itself.

Thus, application security is a must-do in all financial organizations.

Protects the Bank's Reputation

Security Magazine reports that **80% of customers** will be discouraged from using a bank's services if their information is compromised. Moreover, 85% of these customers will share the account of their poor experience with friends and family, further discouraging them from using the bank.

Reputation is of immense importance, especially when it comes to online banking and financial organizations. One breach could leave a negative mark against the bank for years.

To protect the bank's reputation, application security must be prioritized properly to ensure that no form of financial data is compromised in any way.

Prevents FDIC Penalties

The Federal Deposit Insurance Corporation has certain regulations in place that protect customers when their financial institution becomes compromised.

For example, if a bank's website is hacked and the attacker executes transactions in an account-holder's name or credits cash to accounts without permission, the FDIC will cover losses for customers up to $250,000 per account.

However, the FDIC's rules must be followed by the bank in order for the organization to receive services from the corporation. If the bank bypasses or breaks these rules, the FDIC places huge penalties on them for noncompliance.

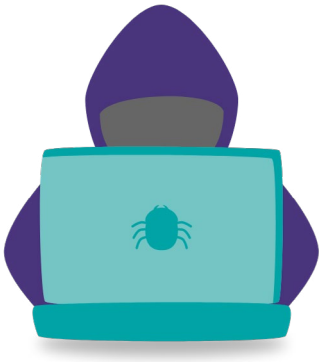
Recovering from penalties can be tough since some of these organizations end up in heavy losses because of the regulation violations. Additionally, it's hard to maintain the customers' trust once they find out about the bank's noncompliance.

Why Are Financial Institutions and Banks Victims of Cybercrime?

However, the FDIC's rules must be followed by the bank in order for the organization to receive services from the corporation. If the bank bypasses or breaks these rules, the FDIC places huge penalties on them for noncompliance.

Recovering from penalties can be tough since some of these organizations end up in heavy losses because of the regulation violations. Additionally, it's hard to maintain the customers' trust once they find out about the bank's noncompliance.

Since banks have access to sensitive information, it's easy to understand why cyber criminals consider them prime targets and are under constant attack by hackers who want to see how far they can get into the bank's system.



Hackers try to exploit vulnerabilities in the software systems of these organizations to gain access and extract data like account holders' names and personal information. They later sell this information to marketers who send out spam emails and market their products on social media.

Banks are striving hard to keep up with technological advances in order for them to be able to stay ahead of cybercriminals. But some financial institutions are still far behind in the road towards top-notch application security.

Here are some ***other reasons*** financial institutions and banks are prime victims of cybercrime:

- **Possess Sensitive Information.** Banks provide access to financial information like customer account numbers, which makes them an easy target for cybercriminals.
- **Lack of Emphasis on Cybersecurity.** Financial institutions often pay less attention to implementingcybersecurity measures and become prime targets for hackers.
- **Use of Third-Party Vendors**. A major reason why most organizations are attacked is that they are too lenient with third-party vendors. Cybercriminals know that financial institutions trust third-party vendors and often let them share login credentials that help attackers gain access to databases.
- **Lack of Robust Systems.** Financial organizations are rarely equipped with robust systems and can be exploited by hackers to breach their network security easily.
- **Lack of Standard Verification Processes.** Various types of sensitive information maintained by financial institutions may be a gold mine for hackers. The absence of a standard verification process makes it easier for cybercriminals to get their hands on such data.
- **Inadequate Monitoring Mechanisms.** Financial institutions should monitor bots and suspicious activities that often occur in their networks to protect online transactions. However, most of them cannot monitor bots or suspicious activity due to inadequate monitoring mechanisms in place.
- **Repetitive Attacks.** Hackers often launch repetitive attacks on the information systems of financial institutions, employing new tactics each time they hit a system. Cybersecurity experts find it difficult to mitigate these multiple and varied threats.

Fortunately, that's where Kiuwan comes into the picture. A global organization providing end-to-end application security solutions, Kiuwan lets you take the DevSecOps approach to code security. You can integrate it with your CI/CD/DevOps pipeline to automate your security processes.

With the world more interconnected than ever before, the security of financial assets becomes an issue not just for individual customers but also for companies looking to expand their services beyond national borders.

According to CSI Web, financial service providers and banks were forecasted to face these cybersecurity threats in 2021.

Supply Chain Attacks

A supply chain attack occurs when a perpetrator manipulates parts or the entire production and distribution process of a company so that their products or software can be maliciously modified.

The targeted company is often unaware until it's too late, and its brand and market share may suffer irreparable damage as a result.

Cloud-Base Attacks

Many organizations use cloud-based services to share and store information. While these platforms offer convenience and efficiency, they can also expose companies' most sensitive data to hackers, as the cloud has proven itself as a vulnerable target for cybercriminals.

Business email compromise (BEC), often referred to as "**CEO fraud**," is a form of phishing that targets employees who have access to financial accounts.

BEC criminals send fraudulent emails to employees of a targeted organization, posing as company executives or other trusted sources.

The messages contain instructions that direct the employee to initiate wire transfers from the company's account to bank accounts controlled by the attackers.

Virtual Private Network Attacks

With remote work becoming popular since the pandemic, many cybercriminals are likely to use VPN attacks to target people on the move.

The attacks are carried out by tricking employees into downloading malicious software that lets the cybercriminal steal valuable data, information, and money.

.

Cybersecurity Risks for Financial Organizations

Financial organizations are always at risk of loss of sensitive data.

Unfortunately, cybercriminals can perform ransomware attacks against financial institutions for huge ransoms without doing much research or spending much time and effort developing their own tools. This is true because they can use readily available tools against any organization with vulnerable Windows servers, even if they don't have an online presence.

Here are some risks financial service providers face:

State-Sponsored Attacks

While it may sound mind-boggling to some, cyberattacks are sometimes encouraged or even launched by foreign governments. State-sponsored cyberattacks are becoming increasingly common.

In 2016, for example two Iranian men were accused of cyberespionage for hacking into networks that controlled critical pieces of infrastructure, including a dam in Rye, New York. The men are being charged with conspiracy and having unauthorized access to protected computers.

State-sponsored attacks are so concerning that NATO has declared cyberspace the fifth domain of warfare. Here are some reasons foreign governments attack a country's financial institutions:

- **Destabilize the Economy.** Cyberattacks are used to steal money as economic sabotage against another country. For example, the Wannacry ransomware attack that struck over 200,000 computers in 150 countries cost companies billions of dollars to recover.
- **Raise Costs.** Cyberattacks can target financial institutions and raise costs for trading and transactions for consumers and businesses. They can also be used to hinder investments by destroying trust in a market or industry.
- **Spy on Financial Institutions**. Governments use cyberespionage to track the spending habits of individuals or corporations with close ties to their countries' governments or to industries that are of interest. In some cases, these groups will pay hackers for information stolen from foreign sources. In other cases, hackers may sell the information they steal from organizations after attacking them.

- **Spread Fake News.** Governments also use tactics in cyberspace to spread fake news about market trends in order to influence the existing trade value. Research from the Yale School of Management showed that article writers had a huge impact on trading behavior in the past. In fact, a fake article was more influential than a real one.

Third-Party Data Breaches

Today, banks have allowed third-party organizations to access their systems for transactional purposes. While this practice has made things convenient for customers, it has also opened a new door for hackers to come through.

Third-party networks are often prone to cyberattacks because they are not as secure as the bank's network.

Since these third-party organizations only have one function, to access databases but not store or monitor them as banks do, hackers can exploit their vulnerabilities and steal data without getting noticed.

Mobile App Vulnerabilities

Since the beginning of 2020, the FBI reported a 50% spike in mobile banking. The authority has also warned consumers about fraud through mobile apps due to the increase in the number of fake apps and app-based trojans.

A Guardsquare analysis from 2019 showed that less than 50% of financial apps on the Android Play Store were using proper mobile application security. As is evident, this is bound to create security risks for consumers.

Since banks are now facilitating mobile banking, they must keep this new avenue secure for their customers. Here are some mobile app vulnerabilities that financial institutions should focus on resolving:

Insufficient Transport Layer Protection

Mobile apps are often treated as less critical applications when it comes to security. Though one can use SSL/TLS to secure mobile apps, some banks may choose not to do so to save costs.

This decision leads to sensitive information transfer in the clear, making it vulnerable to interception and spoofing.

Unencrypted Network Traffic

Apart from SSL certificates, an in-house transport layer security also helps in protecting traffic when it is mishandled by firewalls (like Cisco ASA).

Data stored in the cloud may be encrypted using keys that are directly available with service providers. However, it cannot be considered safe unless data is protected through secure channels while moving over the network.

Poor Authorization Mechanisms

OAuth 2.0 protocol is commonly used for authorization, but it lacks user authentication during the authorization step. As a result, once a user is authorized, they could act on behalf of another.

Password Storage Vulnerabilities

Passwords are stored in plaintext or hashed formats which can be deciphered using simple algorithms. Hackers may use these easily available tools to decrypt the password hashes.

AES encryption with 4 to 6 character-length salts is used to store passwords, making passwords less secure over time. Even though hashing functions like bcrypt and SHA-2 are used to protect stored passwords, they also have their limitations.

They cannot distinguish between an attacker running dictionary attacks against stolen hashes and legitimate users who choose weak passwords for additional protection.

Data Exposure Through Third Parties

One of the biggest issues with applications today is data exposure through third parties. Attackers are looking for ways to access sensitive information through APIs, web services, or mobile apps that have privileged access to critical systems.

Hackers exploit this type of access by intercepting the API calls and relaying them to the real server to extract large amounts of data in a short period.

Insufficient Session Expiration

Sessions that do not expire increase the time for attackers to perform an attack, as they can reuse a stolen session token.

In addition, it is important to set the right session timeout, so users are not inconvenienced if their sessions are hijacked. However, long-lasting sessions increase the window for potential attacks.

Insufficient Logout

Like short session expiration, it is important to ensure that all related tokens and cookies are invalidated across other devices or browsers when a user logs out of their application.

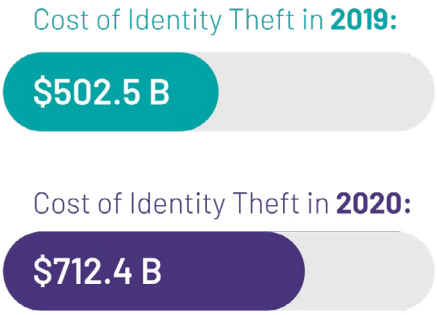
Otherwise, if a user leaves their personal computer open, an attacker could potentially still use the stale and valid session.

Identity Theft

Another cybersecurity threat in the banking and financial service provider space is identity theft.

Hackers use social engineering tactics to gain personal information from unsuspecting victims, allowing account access and the ability to send money through wire transfers. In a few cases in the United States, hackers have used this method to steal funds.

According to the Aite Group, **47%** of Americans were victims of financial identity theft in 2020. Their report, *U.S. Identity Theft: The Stark Reality*, showed that identity theft cost **$502.5 billion** in losses in 2019 and increased by 42% to **$712.4 billion** in 2020.



If a customer learns that someone has been using their name and information to commit crimes and violate laws, they will of course be stressed and frustrated.

The feeling is understandable because they have been dragged unknowingly into a situation of which they want no part. In the process, their reputation may have been damaged, and their social life impacted in negative ways.

According to Experian, 41% of the victims of identity theft experienced sleep disturbances. Meanwhile, **29%** developed physical symptoms, such as heart palpitations, aches, stomach issues, and sweating.

Here are some ways in which identity theft can affect a bank's customer:

Tax Debt

If the attacker assumes a customer's identity, uses their social security number in the job application process, and does not pay taxes on subsequent income earned, the customer can end up with a massive tax bill.

The attacker may also file a return in the customer's name and submit erroneous information. The customer would then have to deal with the aftermath of this mess.

Damaged Credit

If an attacker uses a customer's social security number to open a credit card, bank account, or to buy a car, the customer will have to deal with this unpleasant situation.

The attacker can use the victim's name, date of birth, and social security number to open fraudulent consumer accounts. They can then quickly sell items for cash or run up large balances on credit cards without ever paying them off.

Along with affecting the customer's ability to get a loan or apply for a credit card in the future, this kind of attack could also hurt a victim's job prospects and increase their insurance and auto premiums.

Fraudulent Online Activity

If an attacker gets access to a client's online accounts using their social security number, they can also cause other kinds of serious damage.

They can change billing information so that the monthly bill goes to an entirely different address. If they do this with a bank account, it can lead to checks being written without the client's permission.

With their utility bills, they could end up receiving notices about unpaid service and even be cut off from power or water on occasion.

Criminal Record

More importantly, if an attacker uses the customer's identity to commit crimes and is later caught and brought to justice, the customer will have to disentangle the clean record from the criminal charges. Besides creating stressful situations for the customer, this could also give the bank a bad reputation.

Employee Errors

Cybersecurity risks that involve employees are not always intentional. It's possible that the wrongdoing was completely unintentional. For instance, an employer may open a phishing email that is disguised as an important message from senior management.

When employees are not aware of the cybersecurity risks, they can cause serious data breaches with simple mistakes, like sharing passwords or clicking on dubious emails.

Phishing Attacks

Phishing attacks refer to attempts to obtain sensitive information such as usernames, passwords, and credit card details by deceiving victims into believing that they are communicating with legitimate organizations, such as financial institutions or social media sites.

Phishing attacks can be carried out through email messages, website pop-ups, or instant messaging programs.

The FBI reports that phishing attacks were the most common type of cybercrime in 2020. The number of phishing attacks increased from **114,702 incidents** in 2019 to **241,324 incidents** in 2020.

Phishing is one of the most common methods used to gain unauthorized access to user accounts. In a phishing attack, an attacker typically masquerades as a trustworthy entity — such as a popular social networking site — to steal unsuspecting users' login credentials and potentially lay waste to their entire digital life.

Cloud Servers

Banks and financial institutions often use cloud storage services to host their online content. In this way, they do not need to build or maintain their own servers.

Hackers are adjusting to the cloud trend by targeting these services to gain access to sensitive financial data.

If these cloud servers are not secure, banks can be exposed to unwanted visitors. One of the most common vulnerabilities in cloud storage services is unauthenticated file uploads.

When a hacker can upload files without having to provide authentication, it becomes easy for them to create an anonymous shell account and then access that account using File Transfer Protocol (FTP) or WebDAV.

Cybersecurity *Solutions* for Banks and Financial Service Providers

According to a spending forecast by IDC, banks will invest more in security solutions than any other industry. In fact, the security spending by banks will account for **30% of all security spending in the world**.

Here are some finance and banking security solutions that organizations can implement.

1: Adopt Artificial Intelligence

According to CISCO, the average time companies take to detect threats is 100 to 200 days, which is not even nearly quick enough. Banks can use artificial intelligence tools to identify threats in real time, therefore shorting the detection window to hours or seconds.

Artificial intelligence solutions will also have the ability to learn from past experiences and detect future attacks.

For instance, Kiuwan's flexible licensing options allow financial organizations to choose one-time scans or continuous scanning, depending on how stringent they want security to be.

2: Change Security Posture From Defensive to Collaborative

While **no system is 100% safe**, it is always better to be proactive and prevent an attack than to play catch up with a breach.

Financial institutions can leverage predictive analytics for better change management and security posture. With real-time insights, they can take action earlier and collaborate with stakeholders before the data is compromised or leaked externally.

3: Monitor Cloud Security

The need to monitor file usage on the cloud has become increasingly important with the rise in cyberattacks and data breaches.

Now that banks are using cloud storage services, they are susceptible to attacks from another source.

One way of preventing these attacks is to monitor the cloud. Financial service providers should also ensure they avail cloud services from trusted vendors. Doing this will help strengthen their security posture and maintain the comfort of their consumers.

4: Use Strong Authentication Methods

Authentication methods like multi-factor authentication (MFA) are more secure than passwords alone. They're harder to phish and are always changing. Thus, if a user's credentials are stolen, the hacker won't be able to use them for long.

Here are some benefits of using MFA:

- **Reduces Identity Theft and Fraud.** Since MFA requires two or more pieces of information to log in, it's harder for hackers to breach your account.
- **Reduces Phishing Scams.** Even if a hacker does steal one of the authentication pieces, they won't be able to complete the second part of the 2FA process.
- **Increases Customer Trust.** Customers are more likely to trust banks and other organizations that use an MFA system.

Online businesses need to implement a multi-factor authentication system to keep their customers safe.

5: Implement the Zero Trust Model

The zero trust model is a framework for securely organizing and managing access to resources in a modern, cloud-based world. In this model, an organization never trusts user authentication systems, gateways, or any sort of intermediary.

It means tough decisions have to be made about who needs access to internal resources and in what ways they need access.

According to the NIST Special Publication 800-207, ***"Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero-trust enterprise is the network infrastructure (physical and virtual) and operational policies in place for an enterprise as a product of a zero-trust architecture plan."***

A zero trust model has the following principles:

- All computing services and data sources are resources.
- All communication has to be secured irrespective of the network location.
- Users get access to individual enterprise resources based on per session.
- A dynamic policy determines access to resources. The policy includes different factors, such as application or service, the requesting asset, and client identity.
- All resource authorization and authentication is dynamic. It is also strictly enforced before the user gets access.
- The organization collects sufficient information about network infrastructure, communications, and the current state of assets to improve its security posture.

According to Sanjai Gangadharan, Area Vice President – South ASEAN at A10 Networks, Inc., "***The last principle is the key to making a Zero Trust Model actually work in the real world. By inspecting all traffic, including secured communications using TLS/SSL decryption and inspection (SSLi), financial organizations can track what's coming into their networks and what's trying to get out. Correctly implemented and deployed, SSLi can efficiently and cost-effectively prevent the entry of malware and the exfiltration of sensitive data making the Zero Trust Model robust and complete***."

6: Update System Versions

Finance and banking security is also breached due to outdated system versions. Such organizations should update the version of OS and other software they are using. Doing so helps prevent security vulnerabilities, hampering attackers from entering into their systems and making them vulnerable.

7: Security Awareness

It is essential to foster awareness of security measures and their importance from within the finance and banking industry and its institutions.

Educating employees about security is not an easy task, but it's one of the most important things that organizations can do to improve security.

Staff should be trained to use authentication processes properly, avoid unauthorized downloads, access private information appropriately, and protect themselves from malware, social-engineering attacks and the like.

8: Authorization Process

Organizations should ensure improvement of the authorization process. They should know exactly which users are accessing the system and what they are allowed to do within the organization.

It can help them recognize anomalies in user behavior patterns, e.g., multiple errors being made by a single user who is not supposed to access certain information or a number of failed logins from the same user.

9: Network Boundary Protection

Another banking security solution is to restrict the access to network boundaries which must be implemented using a web application firewall and an intrusion detection and prevention system (IDS/IPS).

By deploying these two applications, organizations can stop zero-day attacks by blocking the source of the attacks and making sure that users with malicious intents cannot enter the corporate network.

10: Increase IT Budgets

Banks and similar organizations should also increase the budget for IT resources to ensure they have enough bandwidth to run the applications they need.

In most cases, companies that experience a data breach require months or even years to recover from it. During this time, customers will probably transfer their business to other financial institutions.

Had the organization allotted an increased and adequate amount on IT needs, it could have avoided suffering the loss of customers and money.

11: Use Reliable Security Solutions

Nowadays, there are many security solutions on the market that financial service providers can use to keep themselves and their customers safe from cyberattacks.

Kiuwan is one of the leading names in this field, providing security solutions for your DevSecOps process. With Kiuwan, you can enjoy fast vulnerability detection. The setup takes just a few minutes, letting you scan and get results instantly.

Plus, you can integrate it with your CI/CD/DevOps pipeline to automate your security processes. The software is immensely helpful for financial organizations that work with third-party services since it remediates vulnerabilities and ensures license compliance.

12: Include Ransomware Threat in the Incident Report Plan (IRP)

The incident report plan refers to documented procedures for reporting an incident, including the roles and responsibilities of those involved. Creating an incident report plan is only part of the process. Ensuring that you communicate this plan to your employees is equally important.

Ransomware is typically transmitted through phishing messages. The messages are sent from email addresses that appear to be legitimate but are not.

Many of them contain an infected file or link that the end-user opens, allowing the ransomware to execute and lock down files. Employees should be trained on how to identify these messages and report them instantly.

Additionally, as a part of the IRP, banks and finance organizations **should be able to answer** certain questions:

- Do you adequately back up your data and systems?
- Do you plan to communicate with stakeholders?
- How do you plan to deal with attackers?

You shouldn't have to answer these questions for the first time in the middle of a ransomware attack. Rather, if you already have answers for them, you'll be able to deal with a ransomware attack more effectively.

13: Implement Application Security

Application security testing means testing web applications for security. Web apps like Gmail, Facebook, and Twitter are well known to the public, but banks and other financial institutions also use web applications for communications with stakeholders.

Banks should not forget application security standards (e.g., OWASP, ISO 27001) that will help reduce organizational risk. A good strategy is to integrate these standards into the development cycle, requiring software developers to execute security testing like static and dynamic application security testing during their development process before handing it over to quality assurance testers.

If banks use a web application to communicate with shareholders, prospects, or customers, they need to make sure it's secure.

14: Raise Customer Awareness

Along with taking necessary payment cybersecurity and application security steps at their end, banks and financial service providers should also make the customers sufficiently aware of the looming cyberthreats.

They can do this by notifying them about the importance of data encryption, raising awareness about phishing emails, and asking them to report any unusual activity on their credit/debit card accounts.

FINAL WORDS

By now, it should be clear that application security and payments cybersecurity is critical for the success of any financial institution.

Such organizations must have dedicated security staff and professionals who can sniff out possible breaches and cyber threats in real-time.

Additionally, they should develop a feasible action plan to keep customers' money and identity safe from attackers.

Kiuwan is a remarkable provider of security solutions that allow organizations to scan their code and identify vulnerabilities. Since it's compliant with stringent security standards, including CWE, OWASP, PCI, CERT & SANS, it's highly dependable and effective.

REQUEST A TRIAL AT KIUWAN.COM/REQUEST-A-TRIAL
LEARN MORE AT KIUWAN.COM

GET IN TOUCH:

Headquarters
2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA

United States **+1 732 895 9870**
Asia-Pacific, Europe, Middle East and Africa **+44 1628 684407**
contact@kiuwan.com
Partnerships: **partners@kiuwan.com**