THE DIGITAL RISK LANDSCAPE:

A REPORT ON TOP FINANCIAL INSTITUTIONS & THIRD PARTY RISK

TABLE OF CONTENTS

TEAM CYMRU™

THE POWER OF PURE SIGNAL™

INTRODUCTION

Today, banks and financial institutions are using more technology than ever to offer their customers and shareholders more value, streamline their internal processes, and stay at the forefront of their industry. Their digital footprint is expanding across the globe and to thousands of third parties.

> **A major cyberattack poses a threat to financial stability."**
>
> **International Monetary Fund, imf.org**

Yet with increased scale and business opportunity comes increased risk exposure as well. Not only can even just one exploited vulnerability result in data theft, financial loss, and reputational damage, it can result in high regulatory fines as well. More often today that risk is coming from third parties.

Unfortunately, many financial institutions may not even be aware of the risks they harbor until after an incident occurs. They may not know the extent of their digital assets, where those assets are located, or if those assets contain vulnerabilities. They're also likely unaware of how using those third-party platforms can introduce risk as well.

> **The significance of cyber risk has certainly been heard in C-suites and boardrooms."**
>
> **World Economic Forum, Global Cybersecurity Outlook 2023**

This research seeks to answer how much cyber risk financial institutions are exposing themselves to today. The goal is to view banking and finance infrastructure from the attacker's perspective, and to discover what they see to potentially exploit and start a cyber attack.

To find out, we analyzed the internet-facing digital assets of five top financial institutions around the globe. The data includes internet domains and IP addresses and their associated vulnerabilities, which offers a window into potential security risks, weaknesses, and the external digital risk landscape for financial institutions.

By looking at this data, we wanted to find out:

- How many and what kind of online risks these banks face with their own digital assets, as well as with third-party assets.
- What are the current third-party risks across the most utilized platforms.
- How much banks and financial institutions rely on other companies (like cloud services) and the risks that come with that.
- What regulations and laws are there to help banks stay safe, and how they affect business operations.
- What banks can do to avoid or minimize these risks.

By the end, you'll have a better idea of the risks banks face by simply doing business in an online, digital world, and what can be done about those risks.

KEY FINDINGS

Overall Risk Exposure:

Nearly 1% of all digital assets contain vulnerabilities, yet for some banks, over 7% of their assets contain vulnerabilities. This underscores the need for stringent cybersecurity measures, as digital assets — especially internet domains and IP addresses — harbor potential security risks from malicious actors who will exploit them once found.

Vulnerabilities Severity Distribution:

68% of identified vulnerabilities had a severity level of 5.00 or higher, meaning most vulnerabilities pose a moderate to critical risk, and their sheer volume can't be ignored.

Large banks are directly and indirectly exposed to data breaches:

We discovered 537 critical vulnerabilities total containing 161 unique vulnerabilities that can result in financial losses due to data breaches, a tarnished reputation, potential legal implications, and a loss of client trust.

Weaknesses in third-party platforms could lead to regulatory and legal consequences:

75% of vulnerabilities are associated with third-party platforms, which can lead to successful compromise of financial systems, financial losses, regulatory fines, and potential lawsuits.

Interconnected global banks share similar risks and vulnerabilities:

Amazon is the third-party platform with the highest number of vulnerabilities, followed by LG Uplus, NTT, and Alibaba. These common third-party platforms bring shared threat vectors that allow a single approach from a malicious actor to be perfected, making them more effective when targeting banking systems and infrastructure.

RESEARCH METHODOLOGY

This research was conducted to gain insight into the digital vulnerabilities of global financial institutions. Our methodology was designed to be both accurate and comprehensive.

Data Source:

- We used Pure Signal Orbit, Team Cymru's own attack surface management platform. This tool accesses Pure Signal, the world's largest data ocean of threat intelligence and digital assets information
- Scanning for assets was extended from our usual 24-hour window to one week, ensuring the most complete picture of assets and vulnerabilities could be achieved.

- The starting point for the five research candidates used their Top Level Domain (e.g., bank.com), and extended outwards.
- To qualify as a candidate, each financial institution had to be within the Top 5 annual revenues for their specific geographic region. No names have been used to ensure anonymity.

Tools and Analysis:

- Unique Identification: For each bank, assets were uniquely identified to ensure no duplication in the data.
- Severity Scoring: We used MITRE's industry standard CVE severity scores to rank vulnerabilities. These scores help in understanding the potential impact of each vulnerability.
- Third-Party Platforms: We assessed the reliance on third-party platforms by each bank, grouped by name, and evaluated the associated risks.

Human Oversight:

- While technology did most of the heavy lifting, as with our standard product offerings, our human analysts ensure data accuracy, especially in attributing assets to the correct financial institution.

PART I:
OVERALL RISK EXPOSURE

Banks and financial institutions face a number of digital risks each day from malicious actors who seek vulnerabilities and will exploit them once found. Weaknesses in internet-facing assets need to be constantly monitored and discovered, as digital assets harbor potential security risk, and the state of risk is fluid, as we'll explore in this research.

What leads to this increased risk for banks and financial institutions in the first place?

The Financial Digital Asset Landscape and Its Challenges

Financial institutions have expanded their online presence exponentially through digital transformation, moving to the cloud, and even customer demand for digital products. Today, a bank or financial institution's digital landscape is comprised of:

Domains and IP Addresses:

These entities serve as the gateways for customers, partners, and even potential adversaries. Understanding the distribution and significance of these assets is crucial for gauging an institution's digital exposure.

Various Global and Regional Assets:

Leading financial institutions have a presence that spans continents. However, digital risks and regulations often vary based on geography, creating potential risk hotspots and regulatory challenges.

Third-Party Dependencies:

Modern banking ecosystems are intricately connected. From cloud service providers to payment gateways, financial institutions rely on a number of third-party platforms to deliver seamless services. But with this reliance comes shared risk.

While this digital sprawl enables banks to reach customers globally through innovative services and products, it presents a multitude of security challenges. It's difficult to secure every system and service in your organization's public cloud infrastructures. Many organizations who use public cloud infrastructures aren't fully in control of their cloud host's security approach, and certainly aren't able to set their own controls to the same extent they would with internal networks. Today, 63% of organizations say they lack centralized control over their third-party relationships — meaning they have no way of knowing what they have access to. And fewer than 1% of companies have visibility into **95%** or more of their assets.

So, if any number of your bank's digital assets had a vulnerability associated with them, would you even know?

Findings: Overall Risk Exposure

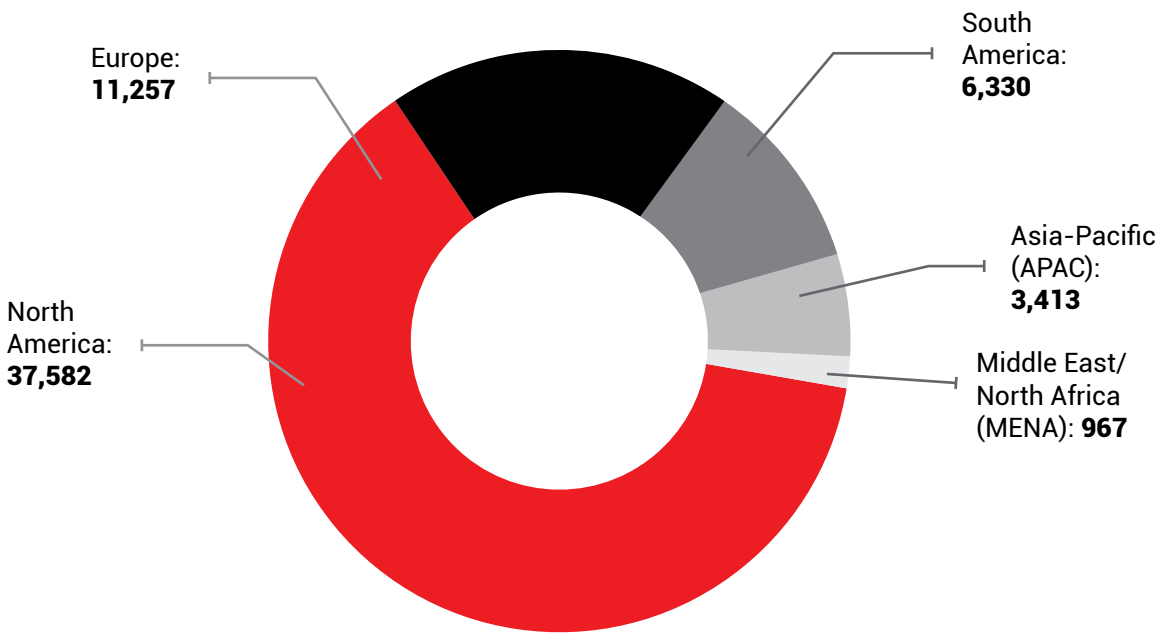
We started with a scan of all digital assets and the vulnerabilities found associated with them in order to get a clear sense of how many assets each bank has and what percentage are impacted.

We scanned 59,549 distinct digital assets from five major banks across the globe.

The total digital assets scanned numbered **59,549**.

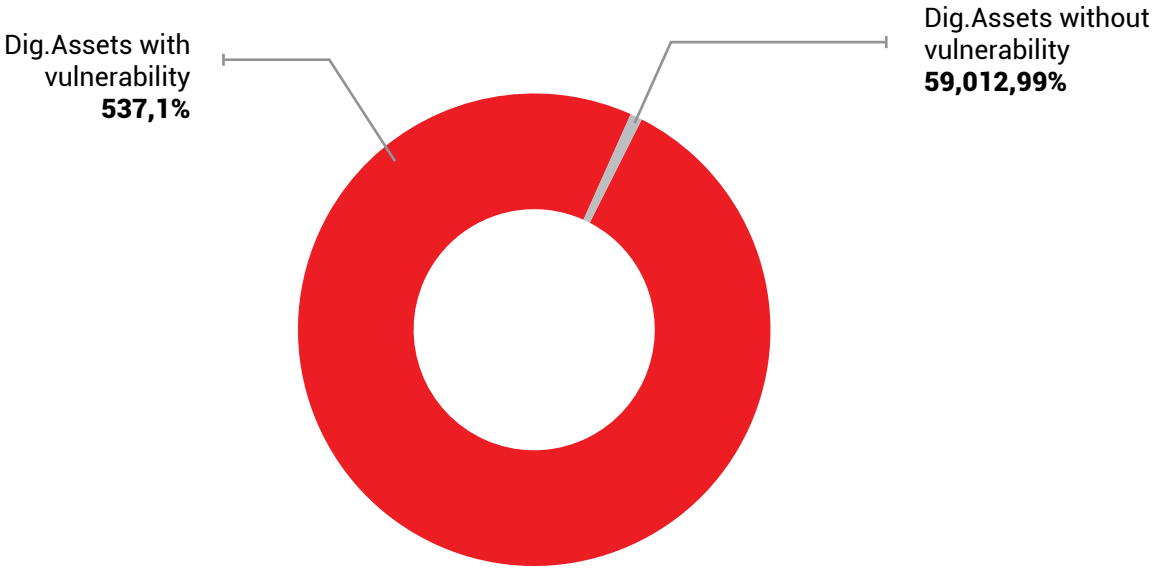
Total digital assets per bank were:

North America:	**37,582**
Europe:	**11,257**
South America:	**6,330**
Asia-Pacific (APAC):	**3,413**
Middle East/North Africa (MENA):	**967**



Nearly 1% of all digital assets contain vulnerabilities, yet for some banks, over 7% of their assets contain vulnerabilities

We found 537 vulnerabilities across those digital assets, and 161 have a unique CVE® ID. Common Vulnerabilities and Exposures (CVE) is a global standard system supported by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Out of our total 59,549 digital assets scanned, 0.90% of those assets contain vulnerabilities.



Here's a breakdown by bank:

BANK	# OF DISTINCT DIGITAL ASSETS	# OF CVES	% OF DIGITAL ASSETS
APAC	3,413	244	7.15%
South America	6,330	74	1.17%
Europe	11,257	123	1.09%
MENA	967	10	1.03%
North America	37,582	86	0.23%

Summary:

Nearly 1% of the total number of digital assets we scanned from five major banks around the world are found to be associated with common vulnerabilities, exposing security gaps that could potentially cause major damage to a financial institution. In looking closer at the number of vulnerabilities per bank, we find that while the North American bank has the most digital assets, they have the lowest percentage of CVEs — likely due to their higher regulatory environment. However, the APAC bank has the most vulnerabilities across their digital assets, with over 7% associated with CVEs.

How Financial Regulatory Compliance Helps Decrease Risk

Our data showed that while the North American bank had the most digital assets of the five, they had the lowest percentage of vulnerabilities associated with those assets. Why? It's likely the regulatory environment in which they operate motivates them to prioritize cyber security controls that safeguard their business.

In a nutshell, the risk of significant fines works to secure banking and financial infrastructures.

Operating within one of the most heavily regulated industries, financial institutions have a number of compliance frameworks they must navigate. As banks and financial entities increasingly rely on external platforms and service providers, the potential for vulnerabilities in these third-party platforms poses a significant risk. Regulatory bodies recognize this and emphasize the need for rigorous third-party risk management practices.

A significant portion of data breaches and security incidents can be traced back to third-party vendors. 98% of organizations do business with at least one third-party vendor that's had a breach. Additionally, malicious attacks on software supply chains have increased 742% since 2019. 27% of third-party breaches were ransomware. No only do you need to secure your own digital assets, but you also need to ensure that your external partners adhere to the same rigorous standards, too.

This is where regulations like the following are geared towards heightened disclosure requirements, continual risk assessments, and safeguarding third party suppliers:

GDPR (General Data Protection Regulation):

GDPR mandates rigorous standards for data handling and security in the EU, emphasizing the importance of safeguarding customer information.

SOX (Sarbanes-Oxley Act):

SOX focuses on corporate transparency and accountability around the integrity of financial information and the systems that store this data.

DORA (Digital Operational Resilience Act):

DORA is a recently approved EU regulation with significant implications for U.S. companies providing financial services within the EU or catering to EU customers.

Securities and Exchange Commission's Public Company Cybersecurity Disclosures Final Rules:

The Securities and Exchange Commission's final rules require the disclosure of material cybersecurity incidents and the periodic disclosure of a registrant's cybersecurity risk management strategy.

PCI DSS 4.0 (Payment Card Industry Data Security Standard):

For any institution handling card payments, PCI DSS outlines robust security measures to protect cardholder data.

BSA (Bank Secrecy Act):

Instituted to combat money laundering and other financial crimes, the BSA requires monitoring and reporting certain types of transactions.

GLBA (Gramm-Leach-Bliley Act):

The new GLBA Safeguards Rule requires financial institutions to implement an information security program that includes sufficient safeguards to ensure the security and confidentiality of customer information against unauthorized access from identified threats.

PSD 2 (Revised Payment Service Directive):

A European directive, PSD 2 enforces strict security requirements for electronic payments.

FFIEC (Federal Financial Institutions Examination Council):

FFIEC provides guidelines and standards for various entities, with a focus on promoting uniformity in the supervision of financial institutions.

Following these regulations can significantly decrease your risk, and guide how you handle, use, and store sensitive customer data. But following regulations alone won't keep your attack surface safe — only robust security tools and active attack surface management can do that.

PART II:
THIRD-PARTY PLATFORMS AND RISK

As our data showed, third-party platforms can contribute immensely to increasing your bank or financial institution's risk. Ultimately, weaknesses in third-party platforms could lead to regulatory and legal consequences, and because of these third-party platforms, interconnected global banks share similar risks and vulnerabilities.

Let's look at more of the risk that third-party platforms impose.

The Benefits of Third-Party Platforms

In the digital banking ecosystem, third-party platforms play a pivotal role in hosting cloud environments, supporting operations, and making digital experiences for customers possible. Some of the benefits that motivate many organizations to leverage third-party platforms include:

Efficiency and Scalability:

Third-party platforms, especially cloud service providers like Amazon AWS or Microsoft Azure offer banks the ability to scale their operations without significant upfront infrastructure costs.

Innovation:

Platforms like Cloudflare or Akamai provide cutting-edge services, allowing banks to leverage the latest technological advancements without in-house development.

Operational Resilience:

Third-party platforms often have robust disaster recovery and business continuity plans, ensuring uninterrupted service.

However, despite the business benefits, 82% of data breaches involve data stored in the cloud — meaning these third-party cloud hosts are not as secure as you may think, or the controls just aren't integrated fully with your IT.

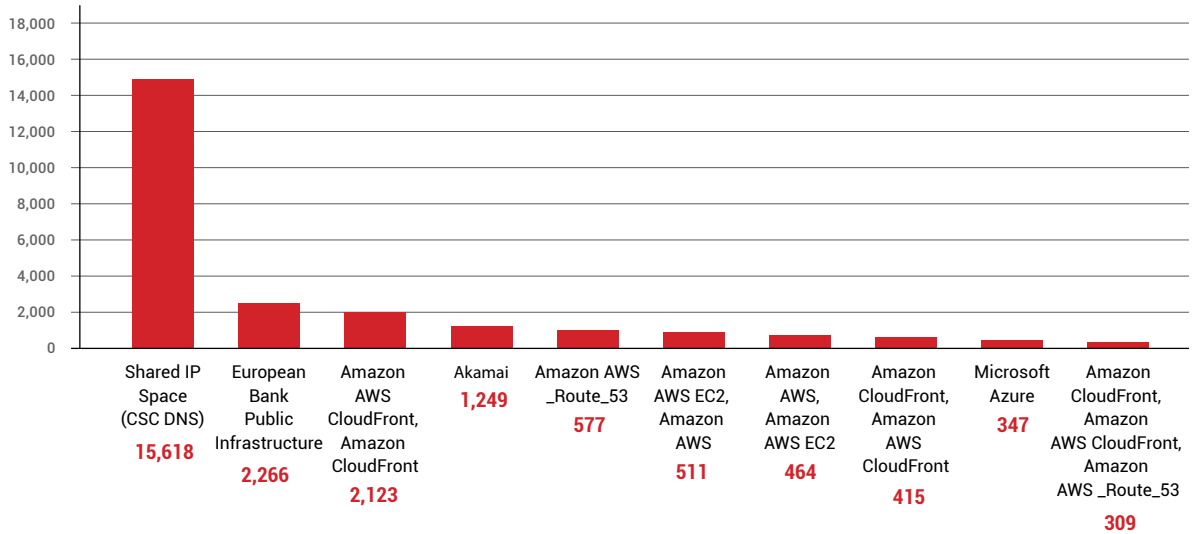
Findings: Third-Party Platforms and Risk

Banks and financial institutions may be taking proactive measures to keep their environments protected, but nearly every organization today works with third-party platforms and services in some way — and it's often hard to know how protected those platforms are.

How much risk are financial institutions incurring by simply using common third-party platforms?

Top 10 most used third-party platforms worldwide

These third-party platforms are used most frequently across all banks, with the number of digital assets associated with them:



Most used third-party platform per bank

The top third-party platform used by each bank is:

North America: Shared IP Space (CSC DNS)

Europe: European Bank Public Infrastructure

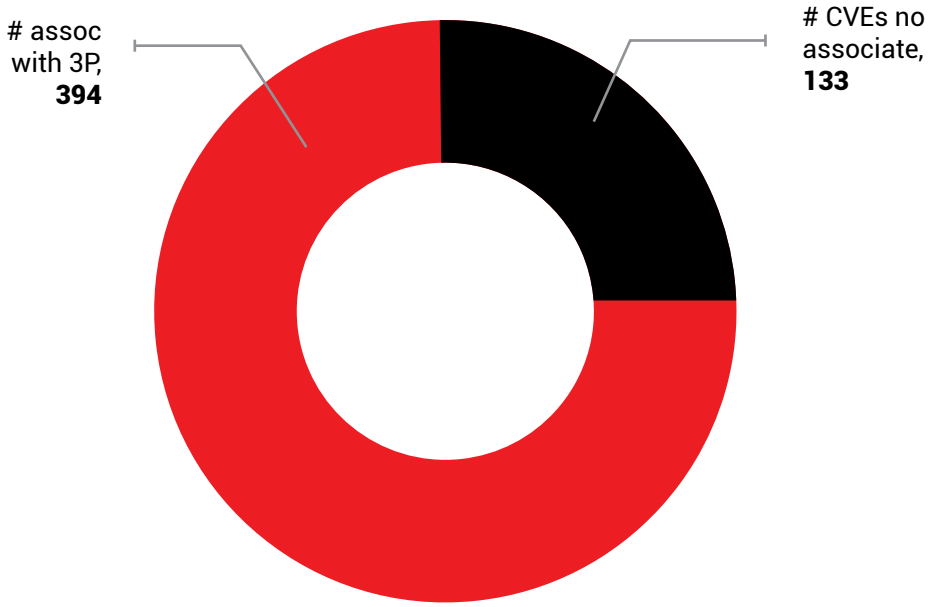
South America: Amazon AWS CloudFront, Amazon CloudFront

APAC: Amazon AWS, Amazon AWS EC2

MENA: Cloudflare

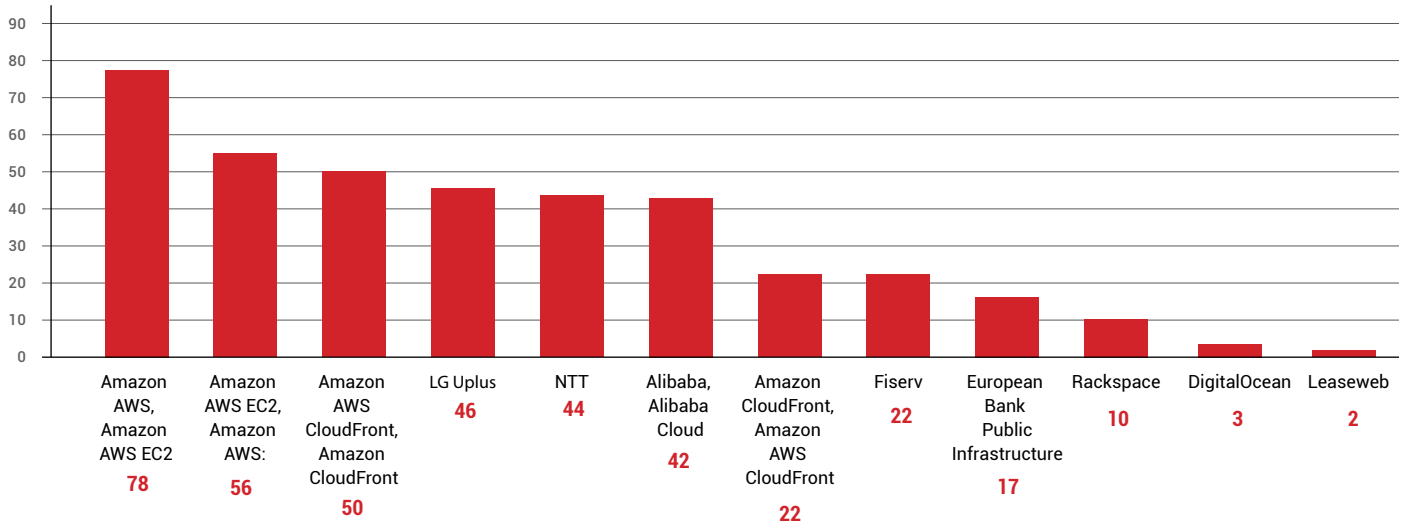
75% of CVEs are associated with third-party platforms

Out of the 537 CVEs uncovered across all digital assets, 394 CVEs are associated with third-party platforms, or **74.8%**. 133 CVEs are not associated with third-party platforms.



Amazon is the third-party platform with the highest number of CVEs, followed by LG Uplus, NTT, and Alibaba

The following are the third-party platforms associated with CVEs, and the number of CVEs associated with them, from highest to lowest:



Notably missing from this list — meaning no CVEs were found associated with them — are the following platforms found in the top 10 list of most used platforms above:

- Akamai
- Amazon AWS route 53
- Share IP Space (CSC DNC)
- Microsoft Azure

Amazon leads with number of CVEs across APAC, North America, and South America, while LG Uplus leads in Europe

When looking at each bank and the third-party platforms they use, here are how many CVEs appear per bank:

APAC (244 CVEs total)

- Amazon AWS, Amazon AWS EC2: 68
- NTT: 44
- DigitalOcean: 3
- No third-party platform associated with CVE: 129

Europe (123 CVEs total)

- LG Uplus: 46
- Alibaba, Alibaba Cloud: 42
- European Bank Public Infrastructure: 17
- Amazon AWS EC2, Amazon AWS: 12
- Leaseweb: 2
- No third-party platform associated with CVE: 4

North America (86 CVEs total)

- Amazon AWS EC2, Amazon AWS: 44
- Fiserv: 22
- Rackspace: 10
- Amazon AWS, Amazon AWS EC2: 10

South America (74 CVEs total)

- Amazon AWS CloudFront, Amazon CloudFront: 50
- Amazon CloudFront, Amazon AWS CloudFront: 22
- No third-party platform associated with CVE: 2

MENA (10 CVEs total)

- No third-party platform associated with CVE: 10

Rackspace has the highest average severity per third-party platform, followed by European Bank Public Infrastructure and Alibaba

The CVEs found on each platform averaged to the following severity, from lowest to highest:

No third-party platform associated	**4.64**
DigitalOcean	**4.95**
Leaseweb	**5.00**
Amazon CloudFront, Amazon AWS CloudFront	**5.79**
Fiserv	**5.79**
NTT	**5.79**
Amazon AWS EC2, Amazon AWS	**5.80**
Amazon AWS, Amazon AWS EC2	**5.83**
LG Uplus	**5.87**
Amazon AWS CloudFront, Amazon CloudFront	**5.90**
Alibaba, Alibaba Cloud	**6.07**
European Bank Public Infrastructure	**6.12**
Rackspace	**7.35**

Summary:

There's a lot of story to tell here about how third-party platforms are associated with the CVEs that were found across these five banks' digital assets, especially the fact that **75%** of CVEs are associated with third-party platforms. Amazon and its associated products lead with the most associated vulnerabilities, followed by LG Uplus, NTT, and Alibaba.

Missing from the list of third-party platforms with CVEs include Akamai, Amazon AWS Route 53, CSC DNC, and Microsoft Azure — all platforms that made the ten most used platforms list. This likely means that these four platforms have robust security measures in place that keep vulnerabilities from happening. CSC DNC is also the top third-party platform used by the North American bank, which is likely the reason why it has the most digital assets yet the fewest percentage of vulnerabilities associated with them.

We also found that the third-party platform with the highest average severity of CVEs is Rackspace, followed by European Bank Public Infrastructure and Alibaba. In our next section, we'll look more at the vulnerabilities we found and their business impacts.

Insights: Top Third-Party Platforms and Their Risk Severity

As our data showed, there's a connection between third-party platforms and the risks from the vulnerabilities we uncovered that can disrupt business operations and impact revenue. It's important to state this does not mean the vendor or their platform are inherently insecure. With many variations of services and platforms, operating systems and infrastructure models, it is not possible to make assumptions that relate to the security or integrity of each.

However, here are some insights into what we discovered.

Amazon's Ubiquity and Risks

As our data showed, Amazon's platforms (AWS, EC2, CloudFront) have the highest number of instances with vulnerabilities. Of course, their dominance in the cloud services market means a broad attack surface. Their high number of vulnerabilities and some of the highest severity scores make them appear as one of the riskiest platforms in terms of banks having full control over securing their assets.

Specialized Financial Platforms Have Risks, Too

Fiserv's presence on the list indicates that even specialized financial platforms face significant digital risks. This suggests that industry-specific solutions don't necessarily mitigate or lead to reduced exposure to vulnerabilities.

Regional Platforms Pose Significant Risks

Platforms like LG's Uplus wireless network and Alibaba Cloud, although not globally dominant, present significant risks. This indicates that regional services can pose unique challenges and vulnerabilities to global financial institutions that utilize them.

Potential for Zero-Day Vulnerabilities

The high severity scores suggest the possible presence of zero-day vulnerabilities. These are previously unknown vulnerabilities that haven't been addressed, and if exploited, they can pose significant risks.

The Business Impact of Third-Party Vulnerabilities

Of the most occurring vulnerabilities, here are the top potential impacts to the business:

Financial Losses:

Many of the discovered vulnerabilities can lead directly to financial losses for an organization. This can be in the form of data breaches (with associated costs for remediation, legal implications, and potential fines), operational disruptions leading to lost revenue, and increased IT costs to restore services or enhance security. Financial fraud due to unauthorized actions also falls under this category.

Reputational Damage:

Unauthorized data access, exposure of sensitive or old data, and operational disruptions can harm an organization's reputation. A damaged reputation can lead to loss of client trust, hamper customer experience, and result in decreased future business opportunities or partnerships. Share value can also dip as a result of a breach, but historically, most large organizations recover from this over time.

Operational Disruption:

Several of the discovered vulnerabilities can cause operational disruptions, be it from unexpected server shutdowns, excessive memory usage disrupting service, or data corruption. Such disruptions not only lead to direct revenue loss from downtime but also increase operational costs and impact overall productivity as resources are diverted to restore services.

Personal Reputation:

Senior Executives can have their personal reputation severely damaged following a breach. One well known example is Equifax's chief security officer, Susan Mauldin, and their chief information officer, David Webb. Both these individuals were forcibly told to resign after Equifax's breach of 143 million customer records. This breach cost the company over $1.3 billion in the post-breach long tail of recovery.

These reasons underscore the importance of cybersecurity not just from a technical standpoint, but also from a business resilience, continuity, and brand trustworthiness perspective.

PART III: VULNERABILITIES SEVERITY DISTRIBUTION

Vulnerabilities can have crippling impact if exploited, resulting in financial losses due to data breaches, a tarnished reputation, potential legal implications, and a loss of client trust. And vulnerabilities with a severity level 5.00 or higher pose a moderate to critical risk, and their sheer volume can't be ignored.

In order to better understand the challenges that banks and financial infrastructures face, let's look at why vulnerabilities exist.

Why Vulnerabilities Exist Within Large Financial Institutions

Large financial institutions, given their size and complexity, often face challenges in maintaining and updating their digital infrastructure, resulting in areas that are left weak or completely exposed to attacker exploits. The following may result in presence of these vulnerabilities:

Legacy Systems:

Many banking and financial institutions rely on legacy systems which are not only outdated but also difficult to patch. Upgrading these systems can be resource-intensive and could lead to potential downtime, which is undesirable in the banking sector, so they're often left alone.

Complex IT Infrastructure:

With multiple systems, servers, applications, and third-party integrations, it's challenging to have a holistic view of the entire digital landscape, leading to potential blind spots — and not having the right security tools for full visibility into your environments can exacerbate this as well.

Rapid Digital Transformation:

In the bid to stay competitive, many banks rush their digital transformation initiatives, sometimes at the expense of thorough security checks.

Third-Party Integrations:

Banks often integrate with third-party vendors for various services. If these third parties don't adhere to strict security practices, they can introduce vulnerabilities.

Resource Constraints:

Even though banks invest heavily in cybersecurity, the sheer size of their operations can strain security teams, leading to potential oversights.

Regulatory Challenges:

While regulations are designed to enhance security, navigating the myriad of compliance requirements can sometimes divert focus from other pressing security challenges.

When it comes to taking action, financial institutions may be making incorrect assumptions about those vulnerabilities. Banks might be aware of some vulnerabilities, but may have assessed them as low risk based on their environment. Or they may have remediation strategies, but implementation might be scheduled for a future date due to operational reasons.

Some vulnerabilities might have been flagged by automated systems, but upon manual review, were deemed non-critical. Whatever the approach, there's more financial institutions can do to better detect and remediate these possible threats.

Findings: Vulnerabilities Severity Distribution

Even just one vulnerability in one asset can cause disruption and harm to a financial institution. The 161 distinct CVEs we found across the five banks are all different ways of compromising an organization and can cause various types of business impact and damage. Let's look more closely at what types of vulnerabilities and exposures these banks are facing, and how severe of a problem they could become.

What are we showing?

Each technical vulnerability is assigned a unique CVE ID. This enables IT to assess the risk (potential impact), and then prioritize according to various attributes (severity). This technical information is then usually paired with business criticality, the more important the asset, the higher the impact and severity, the more likely it will receive the most robust processes to resolve.

Top 6 most common vulnerabilities and their business impact

Even just one vulnerability can lead to compromise. Here are the top vulnerabilities and how they impact business.

#1 CVE-2023-25690: Unauthorized data access or extraction.
Business impact: Financial losses due to data breaches, damaged reputation, potential legal implications, and loss of client trust.

#2 CVE-2022-28330: Access unused memory, introduce malicious code.
Business impact: Data breaches leading to financial losses, regulatory fines, and potential lawsuits from affected stakeholders.

#3 CVE-2022-28615: Unexpected server shutdown.
Business impact: Direct revenue loss due to downtime, increased IT costs to restore services, and potential contractual penalties.

#4 CVE-2022-28614: Disrupt service by using excessive memory.
Business impact: Business disruption, lost revenue from downtime, increased operational costs to restore services, and damaged user trust.

#5 CVE-2022-31813: Disrupt web communications.
Business impact: Hampered customer experience, potential loss of sales or transactions, and increased customer support costs.

#6 CVE-2022-30556: Display old or sensitive data.
Business impact: Breach of confidential data leading to financial losses, damaged reputation, potential legal consequences, and loss of client trust.

The top vulnerabilities by bank

Here are the most occuring vulnerabilities that are found in the digital assets for each bank:

APAC (with 6 instances each):

- CVE-2022-31813 (Disrupt web communications.)
- CVE-2022-26377 (Bypass security measures.)
- CVE-2023-25690 (Unauthorized data access or extraction)
- CVE-2022-30556 (Display old or sensitive data.)
- CVE-2022-28330 (Access unused memory, introduce malicious code.)
- CVE-2022-28615 (Unexpected server shutdown.)
- CVE-2022-28614 (Disrupt service by using excessive memory.)
- CVE-2022-23943 (Overwrite memory, introduce malicious code.)

*Note that these vulnerabilities are all new, from 2022 and 2023.

Europe (with 7 instances):

- CVE-2023-25690 (Unauthorized data access or extraction)

N. America (with 5 instances each):

- CVE-2010-2730 (Memory corruption vulnerability.)
- CVE-2010-3972 (Memory corruption vulnerability.)

S. America (with 4 instances each):

- CVE-2022-28614 (Disrupt service by using excessive memory.)
- CVE-2021-34798 (Disrupt server operations.)
- CVE-2022-30556 (Display old or sensitive data.)
- CVE-2022-28615 (Unexpected server shutdown.)
- CVE-2022-31813 (Disrupt web communications.)
- CVE-2021-39275 (Expose system details, introduce malicious activities.)
- CVE-2022-28330 (Access unused memory, introduce malicious code.)

MENA (all with 1 instance):

- CVE-2021-25216 (Vulnerability in servers.)
- CVE-2018-5741 (Inability to write or configure rules.)
- CVE-2021-25220 (False information being returned to clients.)
- CVE-2020-8616 (Potential to exploit server.)
- CVE-2018-5744 (Memory leak.)
- CVE-2022-38177 (Memory leak.)
- CVE-2022-38178 (Memory leak.)
- CVE-2018-15919 (Detects existence of users on a target system.)
- CVE-2018-15473 (User enumeration vulnerability.)
- CVE-2020-8625 (Vulnerability in servers.)

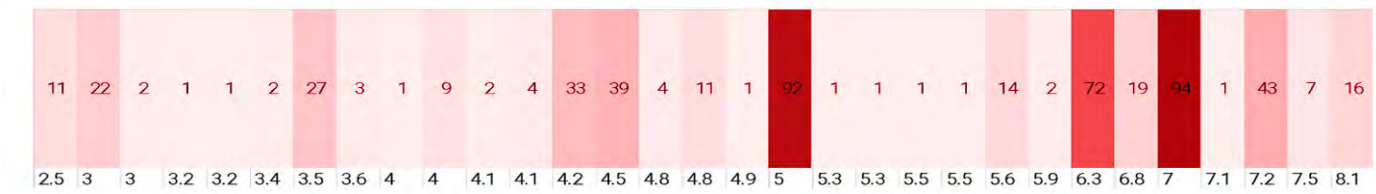
*Note that these vulnerabilities are older, from 2018 to 2022.

One observation about the above findings is that it's likely that one asset has multiple vulnerabilities. These are usually assets that have been missed off an asset register, or simply haven't been discovered using the bank's current methods.

The largest segment of vulnerabilities ranks with a 7 severity

What's the severity of the CVEs found? The largest segment of CVEs (94) ranked with a severity of 7, while 92 CVEs ranked with a 5 severity, and 72 ranked with a 6.3 severity.

Overall, 364 CVEs, or **67.8%**, are ranked with a severity of **5 or higher.**



Summary:

Not all vulnerabilities are the same, and this section clearly shows that banks and financial intuitions aren't just dealing with one type of threat to their organization. With the top six most common vulnerabilities, financial institutions can experience:

- Unauthorized data access or extraction
- Attacks accessing unused memory and introducing malicious code
- Unexpected server shutdowns
- Disruption of service by using excessive memory
- Disruption of web communications
- Attacks displaying old or sensitive data

These impacts can lead to financial losses due to data breaches, damaged reputation, potential legal implications, loss of client trust, regulatory fines, direct revenue loss due to downtime, increased IT costs to restore services, potential contractual penalties, and increased customer support costs.

Banks and financial institutions also have to consider the severity of these CVEs as well. Every organization's risk appetite is different, yet the largest segment of CVEs (94) have a severity score of 7. 364 CVEs — or 68% of the total CVEs — are ranked with a severity of 5 or higher.

What can banks do to protect themselves, why are third-party platforms so concerning, and where do vulnerabilities come from in the first place? We'll take a look at that in the next section.

Insights: Vulnerabilities and Their Risk Severity

As our data showed, not only are vulnerabilities present and prevalent across the banks we scanned, but they can greatly impact that organization as well. Here are some of the insights found when looking at these vulnerabilities.

High-Severity Vulnerabilities are Prevalent

92 identified vulnerabilities, or 17%, have a severity level of 5.00. This suggests that while these vulnerabilities pose a moderate risk, they are not the most critical ones that could be encountered. However, their sheer volume means they cannot be ignored, and typically each of these should be addressed promptly to reduce the potential successful attack.

Overall, despite offering the convenience of outsourcing and cloud-hosted platforms, these systems remain exposed with level 5.00 blended with potentially high impact vulnerabilities — this is likely, given that 68% of vulnerabilities are scored 5:00 or above.

The Uniformity of Severity Scores Implies Shared Risk

As our data showed, the CVEs we found each have a different severity factor, and many share the same severity factor. A severity score of 8.1 across many platforms suggests a shared vulnerability type. This might be due to widespread use of specific software or shared technologies with recognized vulnerabilities.

There are Indications of Well-Maintained Platforms

Surprisingly, the top third-party platforms like Shared IP Space (CSC DNS), Akamai, Amazon AWS Route 53, and Microsoft Azure don't have vulnerabilities directly associated with them in the dataset. This could suggest that these platforms, while extensively used, might have robust security measures in place.

A Vast and Varied Vulnerability Landscape

The dataset contains 161 unique vulnerabilities, indicating that financial institutions face a vast and varied landscape of potential threats. This underscores the need for comprehensive vulnerability management programs that are strategic — organizations must accept that attackers see them as a single entity target, and not divisions and subdivisions like the organization's structure.

Varied Asset-to-Vulnerability Ratios

Institutions like the APAC bank have a higher proportion of vulnerabilities relative to their digital assets (7.15%) compared to others like the North American bank (0.23%). This disparity suggests that while some banks may be more effective at securing their digital assets, others might benefit from enhanced cybersecurity measures.

Potential Delays in Patch Application

The recurrence of vulnerabilities associated with widely-used software like the Apache HTTP Server indicates that there might be delays in applying patches or updating to newer, more secure versions. Legacy systems, operational constraints, or even a lack of awareness could be factors contributing to this delay.

PART IV:
WHAT BANKS CAN DO TO AVOID OR MINIMIZE THEIR THIRD-PARTY RISKS

Banks and financial institutions today have great opportunities for bringing more value to customers through digital transformation and growth. Yet with that growth comes risks. As more organizations adopt cloud environments, as more of their teams go remote, and as they scale across the globe, they're introducing more security risk through their expanding attack surface.

As our data showed above, upwards of 7% of a bank's digital assets could have vulnerabilities ready to be exploited, and 75% of the vulnerabilities we found are associated with third-party platforms. The most prevalent vulnerability we found can result in unauthorized data access or extraction, leading to financial losses due to data breaches, damaged reputation, potential legal implications, and loss of client trust. Overall, we found the most vulnerabilities associated with Amazon, a global trusted third-party, yet we also found vulnerabilities associated with regional and specialized platforms as well.

What steps can financial institutions take to keep themselves aware and protected?

1. Embrace Digital Asset Discovery

The first step in greater attack surface protection is knowing what digital assets you actually have and what risk they pose to the organization. Having better security tools that can monitor and manage your attack surface can give you greater visibility into your asset inventory, and can offer passive discovery of their own and third-party assets. Such non-intrusive methods ensure comprehensive visibility without overstepping boundaries.

For example, the data we used above was performed with Pure Signal Orbit's Third-Party Risk Management tool — which can give you these same insights into your extended supply chain and business partners' digital assets, without the disruption a formal process would entail.

2. Understand, Prioritize, and Address Third-Party Risk

Beyond discovery, understanding the risks posed by third-party assets and why they might impact your organization enables proactive mitigating measures. Whilst the source of the data may be IT related, it's strategically important to translate these into business level metrics. Some areas where the business stakeholders can apply budget and resources to better measure and manage risk include:

Extent of Corporate Reliance:

Understand the reliance you have on third-party platform integrations, be it for hosting solutions, payment gateways, or customer relationship management. What is optimal? What are the risk tolerances?

Risk Profiles:

Whether it's a potential data breach, service disruption, or regulatory non-compliance, assess the risk profile of each third-party dependency. Does the data map to your vendor/supplier terms to apply baseline security controls?

Risk Management and Mitigation:

Create a strategy to manage risk that includes continuous monitoring, periodic assessments, and effective mitigation measures. Does IT provide up-to-date insights to assist with dynamic decision making?

Potential Risks During Integration:

While these platforms have stringent security measures, integrating with them can introduce vulnerabilities if not done correctly. Has IT presented a detailed plan to support the business objectives? Are the risks known and quantified?

Regulatory and Compliance Issues:

Banks need to ensure that third-party platforms comply with all relevant regulations, especially around data protection. Does the supplier questionnaire align with business risks and threats? Do the corresponding terms the vendor or supplier sign up to support the corporate IT security requirements?

Transparency and Reporting:

Comply with the regulations that mandate reporting of third-party data breaches or security incidents. Have workflows and processes been documented to support this, and can the IT solutions and services help meet these requirements?

Operational Resilience:

Many nation-states classify financial institutions as part of their Critical National Infrastructure, and regulators expect banks to ensure continuous service, even in the face of third-party service disruptions. Has IT made provisions for this data to be shared outside their environment, and is it easy to consume for business stakeholders?

3. Improve Regulatory Adherence with Visibility

With regulatory bodies emphasizing the importance of third-party asset visibility, it's more crucial than ever to have a real time view into the risks your third-party platforms pose to your organization. Again, investing in security tools that allow you to monitor your third-party partners and even your supply chain can allow you to see a potential compromise before it impacts you. This can also allow you to see if your third-party partners are putting you at regulatory risk as well. These platforms have matured to ensure value to both IT and business stakeholders, removing many excuses that could prevent organizations from investing.

4. Transparent Communication

Having better tools to provide visibility into your environments and alert you to possible threats isn't the only approach you can take to improving your security. Increasing your communication around security postures, potential risks, and mitigation strategies can foster collective resilience across the supply chain and third parties as well. Being able to articulate business risk and impact of potential threats in business language can help increase leadership buy-in and investment in security improvements.

5. Incident Preparedness

If one of your unknown vulnerabilities is exploited and you experience a data breach, do you know how to respond? Having a well-defined incident response and recovery strategy, bolstered by insights from vulnerability assessments, ensures agility in the face of security breaches. This includes having a playbook of defined roles and actions, and practicing that playbook so that when an incident occurs, you'll quickly stop it.

CONCLUSION

As financial institutions aim to harness the full potential of the digital realm, you must also be equipped to navigate its challenges. Having a holistic understanding of your digital landscape, especially third-party assets, is no longer optional — it's imperative. This can only be achieved by having the right security tools that can give you proactive management of your attack surface, visibility into your digital assets and their vulnerabilities, and insights into your third-party risk. Only then will you be able to take action to proactive protect your organization, your data, and, most importantly, your customers.

Pure Signal™ Orbit

CASE STUDY