B.B. Banks

Elijah Birk | Laura Herman Childs | Ken Kuruce | Shae Smith

TOC

Financial Industry Summary

The financial industry is highly targeted for an obvious reason: whether or not attackers have a specific target area, they also typically want or need money. Per the 2020 DBIR, 91% of attacks in this industry are financially motivated.

Attackers that want data also have a boon here because finances require a significant amount of ancillary data to operate. Per the 2020 DBIR, 63% of attacks were data motivated. The other metrics of attackers are internally financially motivated actors (18%) and errors by internal actors (9%).

Web Applications are just above Miscellaneous Errors as the most common breach source in this industry, accounting for 81% of breaches.

Attacks	**2020**	**2019**	**2018**
Data Motivated (external)	63%	72%	93%
Internal Financially Motivated	18%	36%	7%
Internal Errors	9%	N/A	N/A

Security Challenges in the Financial Industry

- 86% of breaches across all industries in 2020 were financially motivated. This means that the financial industry is highly targeted and must keep up against increasingly large and skilled threat actors.

- Web Applications are significantly used in the financial industry, both for connecting consumers with their own data and for internal operations. This usage only continues to increase as the online world grows, especially in the wake of Covid. Attacks grow alongside this, with web application attacks increasing by 38% in 2021. The growth of web application security is struggling to keep up.

- The financial industry struggles with a significant business need to handle a lot of sensitive information while keeping it secure. With financial and regulatory pressure, there is a lot of desire to get work done quickly and for everyone to have hands-on whatever they need to get that done. The most common error in 2020 was misdelivery. The financial industry struggles with concepts of least privilege and network and administrative security that could limit these mistakes.

Functional Areas: Application Security

Application Security is significant for B.B. Banks as over 30% and the most common of the breaches from the 2020 DBIR related to web applications.

- As the DBIR 2020 highlighted that the financial sector is a crucial playground for financially motivated actors, a web application firewall can help mitigate vulnerabilities, including SQL injection and cross-site scripting (XSS).
    - *Suggested tool:* *Azure Web Application Firewall*
- Email Security is another tool that can be utilized to improve application security. Phishing is just one of the tactics that accounted for significant losses in 2020 ($1.8B). Protecting email security is imperative to maintain customer data as well as the Bank's reputation.
    - *Suggested tool:* *Armorblox Email Security*

Functional Areas: Identity Authentication and Access Management

Dealing with highly confidential information, such as personal and business finances, requires assurance that only the correct people are able to log in and access the correct information. Misuse and inappropriate access controls pose severe consequences.

- Ensure identity authentication so that information remains confidential only among the intended resource(s). This is crucial to maintaining B.B. Banks' business and operations.
    - *Suggested tool:* *Ping Identity,* Multi Factor Authentication
- B.B. Banks develops and implements strict access control tools and privilege management to manage all user accounts, particularly those at high-risk.
    - *Suggested tool:* *CyberArk,* Privilege Management and Access Control

Functional Areas: Training and Audit

Policy, Audit, E-Discovery, and Training are significant for B.B. Banks primarily because our users are more likely to handle data across all verticals, and security needs to be consistent across the entire company.

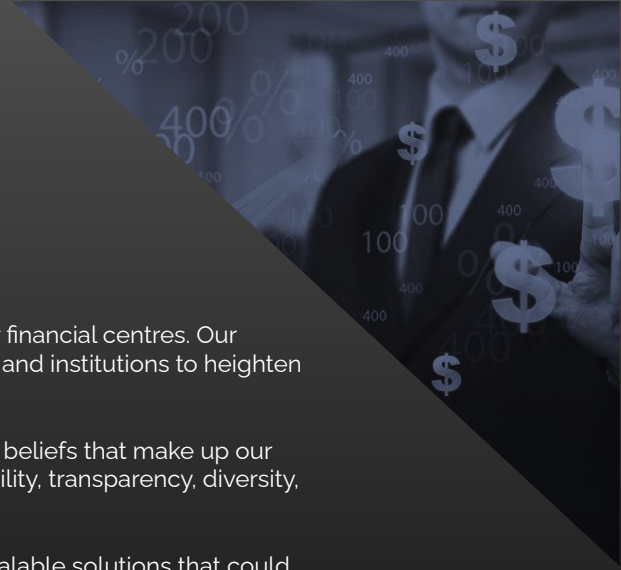
- The 2020 DBIR recommends security awareness and training as a primary defense in the financial industry. This helps teach developers to be careful with their designs and helps ensure every other user handling sensitive data is a bit more careful and considerate.
    - *Suggested tool:* KnowBe4's Enterprise Awareness Training Program
- Audit frameworks are also significant for B.B. Banks to help review our systems to identify misconfigurations and ensure processes involving sensitive information are following our security and privacy standards to minimize opportunities for error.
    - *Suggested tool:* Tandem audit management software

Functional Areas: Systems Administration

Systems Administration plays one of the most critical roles in B.B. Banks' security and data protection. Sys admins are our gatekeepers, ensuring that our servers, internal systems, and networks are maintained and kept safe from security threats.

- The 2020 DBIR recommends boundary defense as part of a multi-layered approach to defense. Layered security controls like Multi-factor Authentication (MFA) and Network Isolation/Segmentation are recommended to reduce the risk of unauthorized access and data and identity theft.
    - *Suggested tool:* Hysolate isolated workspace
- Administrator Audit Trails are a powerful tool used by B.B. Banks to certify that configurations of systems, databases, and applications remain secure. Audit trails also promote accountability and transparency and can help detect intrusion attempts.
    - *Suggested tool:* Wiz for cloud server configurations

B.B. Banks



B.B. Banks is a leading global financial institution and maintains offices worldwide in all major financial centres. Our nearly 40,000 colleagues work together with the world's leading businesses, entrepreneurs, and institutions to heighten economic progress and propel people, technologies, and ideas toward success.

B.B. Banks knows that the way our colleagues think, feel and act is guided by the values and beliefs that make up our culture. Our goal is to manifest those values through service excellence, integrity, accountability, transparency, diversity, and collaboration. With 40,000 employees, this will take some work.

Our organizational size and culture forces us to take a multidisciplinary approach and find scalable solutions that could be delivered globally, either in person or remotely. Our goal is to make sure that everyone has a clear understanding of their role in creating and maintaining a cybersecurity culture and keeping the Bank's information and systems secure.

We are large enough to have our own substantial security operations. However, cyber security impacts every aspect of B.B. Banks' supply chain, so many capabilities will be outsourced to address risks associated with software, assets, and vendors.

Modifying security operations involves identifying gaps between needs and existing capabilities, and this process could result in slower or failed responses. Specialized skills are constantly required to understand the ever-evolving threat environment, so additional staffing may be necessary.

Training on any new security capabilities will be essential. With the size of our organization, we will need a system for routine training and education across all verticals.

References

1. "11: Secure Configuration for Network Devices, Such as Firewalls, Routers and Switches." CSF Tools - The Cybersecurity Framework for Humans, 2 May 2021, https://csf.tools/reference/critical-security-controls/version-7-1/csc-11/.

2. "12: Boundary Defense." CSF Tools - The Cybersecurity Framework for Humans, 2 May 2021, https://csf.tools/reference/critical-security-controls/version-7-1/csc-12/.

3. "About Us." Goldman Sachs, https://www.goldmansachs.com/about-us/index.html.

4. Chapagain, Sinij. "Role of WAF in Core Banking Applications." LinkedIn, Digital Network Digital Network, 29 Apr. 2022, https://www.linkedin.com/pulse/role-waf-core-banking-applications-dnsnepal?trk=pulse-article_more-articles_related-content-card.

5. Gregory, Jennifer. "One Size Does Not Fit All Organizations." Security Intelligence, 9 June 2022, https://securityintelligence.com/articles/cybersecurity-one-size-organization/.

6. Mairs, Tom. "3 Email Security Best Practices for the Financial Services Industry." SparkPost, 15 Oct. 2018. https://www.sparkpost.com/blog/3-email-security-best-practices-financial-services-industry/.

7. Ray, Terry. "Financial Services: Web Application Attacks Grow by 38% In First Half of 2021." Imperva, 19 Aug. 2021, https://www.imperva.com/blog/financial-services-web-application-attacks-grow-by-38-in-first-half-of-2021/.

8. Verizon. "2020 DBIR Results & Analysis." Verizon Enterprise, 19 May 2020, https://www.verizon.com/business/resources/reports/dbir/2020/results-and-analysis/.

References: FA Tools

1. "Audit Management Software." Tandem, https://tandem.app/audit-management-software.
2. "Azure Web Application Firewall (WAF) ." Cloud Computing Services | Microsoft Azure. https://azure.microsoft.com/en-us/products/web-application-firewall/.
3. "Enterprise Security Awareness Training." *KnowBe4*, https://www.knowbe4.com/en/products/enterprise-security-awareness-training/
4. "Isolated Workspace-as-a-Service." Hysolate, https://www.hysolate.com/product/.
5. "Multi-Factor Authentication Solutions ." Identity Security for the Digital Enterprise | Ping Identity, https://www.pingidentity.com/en/platform/capabilities/multi-factor-authentication.html.
6. "Privileged Access Management (PAM) ." CyberArk, https://www.cyberark.com/products/privileged-access-manager/.
7. "Stop Email-Based Financial Fraud." Armorblox | Industry Brief | Financial Services, 2021, https://assets.armorblox.com/f/52352/x/7b16fc6e28/armorblox-financial-services-industry-brief-2021.pdf.
8. "Wiz | Secure Everything You Build and Run in the Cloud." Wiz.Io, https://www.wiz.io/.