CYBLE®

REPORT

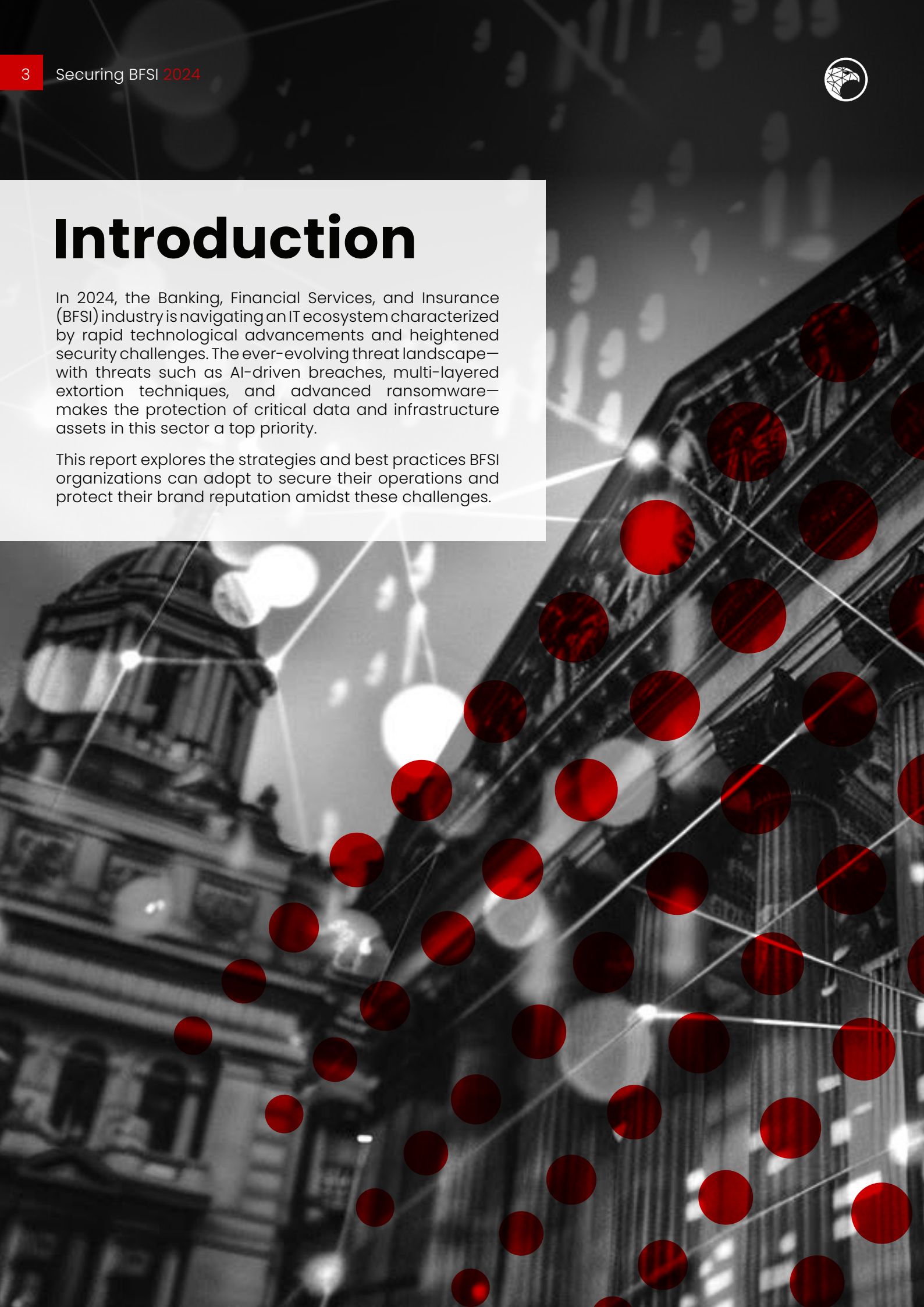
Securing BFSI: An Integrated Approach to Cybersecurity and Brand Protection

Table of Contents

Introduction

In 2024, the Banking, Financial Services, and Insurance (BFSI) industry is navigating an IT ecosystem characterized by rapid technological advancements and heightened security challenges. The ever-evolving threat landscape—with threats such as AI-driven breaches, multi-layered extortion techniques, and advanced ransomware—makes the protection of critical data and infrastructure assets in this sector a top priority.

This report explores the strategies and best practices BFSI organizations can adopt to secure their operations and protect their brand reputation amidst these challenges.



The BFSI Ecosystem: Challenges and Opportunities

The BFSI sector is uniquely susceptible to a myriad of cybersecurity threats due to its reliance on sensitive data, significant assets, and interconnected users. Key issues include:

Supply Chain Vulnerabilities

Increasing reliance on third-party providers introduces single points of failure, making supply chains a significant point of vulnerability. For example, Allianz Global Risks U.S. Insurance Company's 44,000 customers had their PII exposed in the wider MOVEit transfer hack which actually took place at its business partner Enstar. But the entire supply chain was impacted due to this vulnerability.

Cyble has observed an extremely high number of attacks (138,730) targeting CVE-2020-11899. This improper input validation in IPv6 bug allows attackers to remotely execute code via flaws in the commonly used Microsoft Dynamic Link Libraries.

Privacy, Protection, Regulations and Reporting

The widespread use of data analytics and personalized financial services necessitates robust data protection mechanisms to safeguard sensitive information. Stricter regulatory requirements in regions like the US and Europe compel organizations to enhance their compliance and reporting capabilities.

Compliance frameworks such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and country-specific regulations like India's Information Technology Act or Dodd-Frank and FINRA in the U.S. set high standards for data protection and breach reporting in the financial sector. However, staying compliant with these evolving regulations is a challenge, as non-compliance can lead to heavy fines and reputational damage.

Furthermore, BFSI institutions are under constant pressure to ensure that their cybersecurity protocols align with global standards such as the NIST Cybersecurity Framework and ISO 27001, which set guidelines for risk management and best practices in cyber defense. The focus is not only on preventing data breaches but also on ensuring operational resilience during and after cyber incidents.

Cloud Migration

With the shift towards cloud technologies for operational efficiency, BFSI organizations must prioritize cloud security. Misconfigurations in cloud environments, data breaches due to inadequate access controls, and a lack of proper encryption can lead to significant data compromises. According to IBM's 2023 Cost of a Data Breach Report, misconfigured cloud settings were responsible for 19% of breaches in financial institutions.

Attack Surface Expansion

The integration of machine learning, cloud technology, and the Internet of Things (IoT) provides avenues for innovation but also increases the potential points of attack.

A comprehensive attack surface monitoring tool enables quick identification and resolution of vulnerabilities that could lead to data breaches. By implementing such a tool, financial institutions can enhance their security defenses while also meeting the rigorous cyber resilience standards required by most regulatory frameworks.

Cyble has introduced a proprietary attack surface management solution tailored to address the specific cybersecurity challenges and compliance needs of the financial sector.

Facts and Figures

In the past one year, the BFSI sector has witnessed an increase in cyber threats, as financial institutions continue to face complex attacks. Some of the latest statistics highlight significant trends and risks:

- Financial institutions were the **second most impacted sector** based on the number of reported data breaches, experiencing **566 breaches**, leading to over **254 million leaked records**.
- **Data breaches** cost the finance sector an average of $5.9 million, **the second highest cost** among all sectors.
- **Ransomware** remains one of the **top threats to BFSI** organizations, with incidents increasing 13-fold during the second half of 2023 compared to the beginning of the year. Despite 78% of businesses feeling prepared, nearly 50% still fell victim to ransomware attacks.
- **Phishing attacks** poses a considerable risk, with over **711 incidents reported alone in India's BFSI sector** in the last year. These attacks primarily target financial institutions to gain access to sensitive information.
- **Identity theft** accounted for 22% of data breaches in BFSI, with total losses exceeding $6.4 billion.
- **Unauthorized network scanning and probing** incidents topped the list of cyber threats, with over **439,431** such incidents reported. This method is often used by attackers to detect vulnerabilities in financial systems before launching more severe attacks.
- **APT campaigns** targeting BFSI have risen by 30%, costing an average of **$6.5 million per breach**.
- **Vulnerable services** accounted for **54% of all cyberattacks**, enabling malicious actors to exploit weaknesses in financial institutions' networks. This highlights the growing concern over third-party services and cloud-based infrastructure that expand the attack surface.
- **Artificial intelligence (AI)** and automation are playing a critical role both in cyber defense and cybercrime. Threat actors are increasingly leveraging AI to automate attacks and scale operations, while BFSI institutions are using AI for anomaly detection and predictive analytics to pre-emptively identify threats.
- Number of cyber incidents targeted at the financial sector worldwide, has seen a steady rise in the last 10 years.

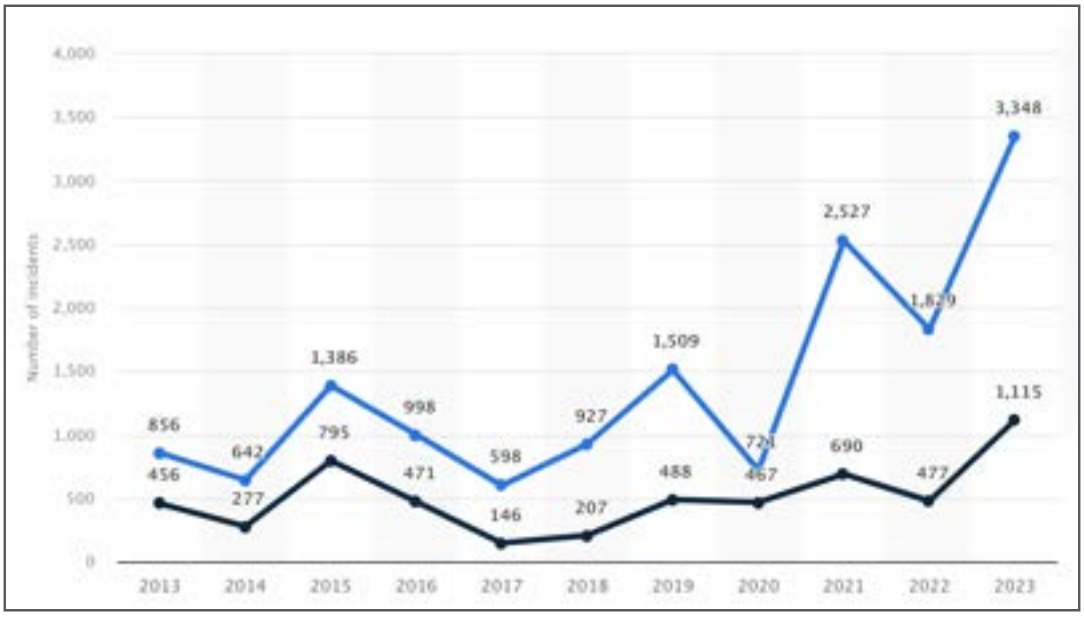


Figure 1. Number of cyber incidents in the financial industry worldwide in the last decade. (Source: Statista)

Enhancing Security Operations Center (SOC) Capabilities

To mitigate these risks, it is essential for BFSI organizations to enhance their SOC capabilities. However, this must be achieved in a cost-efficient manner. Key strategies include:

Hybrid Resourcing Model

Partnering with Managed Security Service Providers (MSSPs) like Cyble, or adopting a hybrid model allows BFSI firms to tap into specialized expertise while retaining strategic control over critical security functions. This model also supports scalability, enabling organizations to quickly respond to new threats without the overhead of maintaining large in-house teams.

Advanced Technological Integration

Integrating machine learning into SOC operations enables faster identification of anomalous behavior. By continuously analyzing patterns across the network, AI-powered systems can detect subtle deviations that might indicate an attack in its early stages, allowing for proactive mitigation. Predictive analytics can also help BFSI organizations anticipate attack vectors and strengthen defenses before threats materialize.

Continuous Monitoring and Incident Response

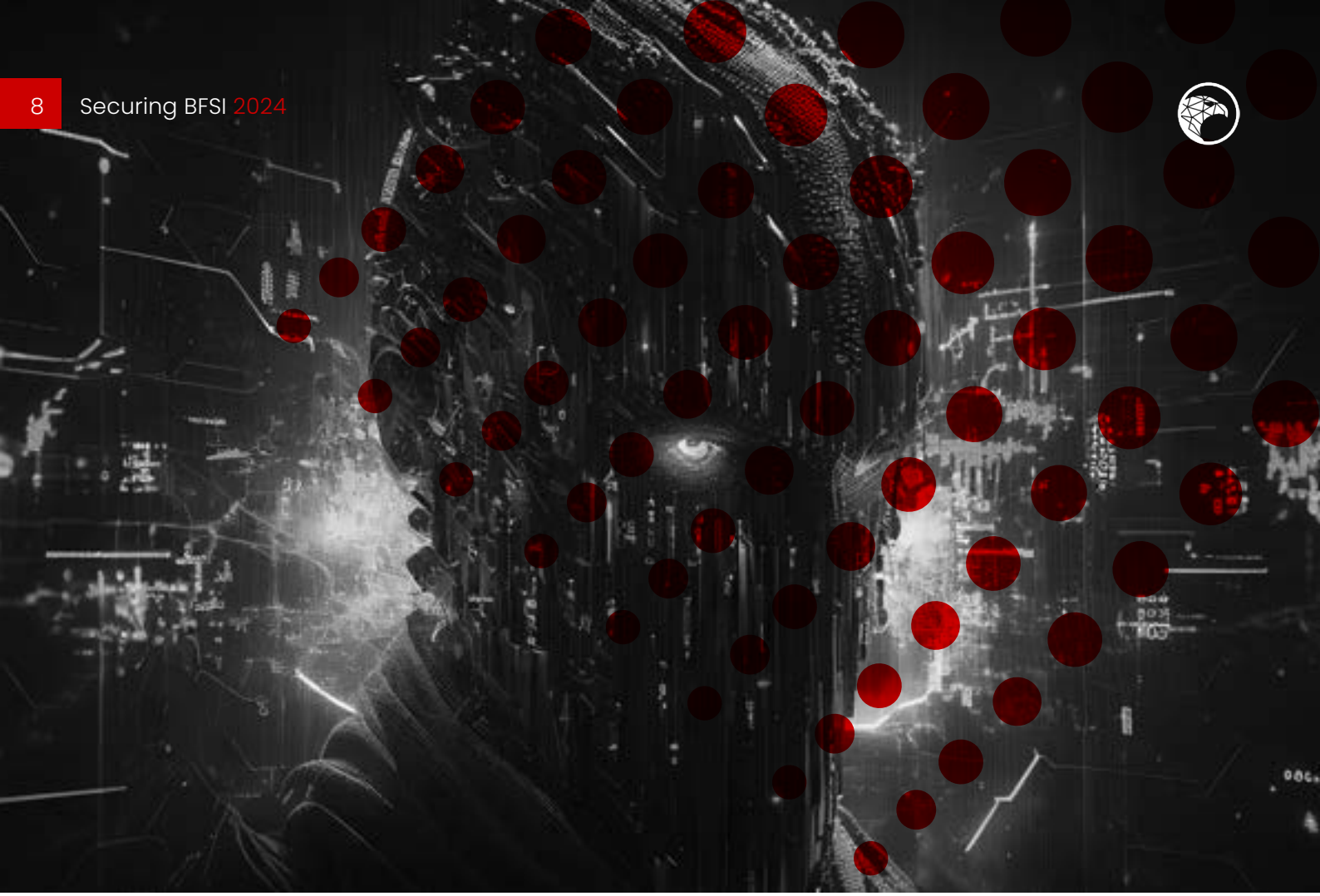
Given the constant threats faced by BFSI entities, continuous monitoring is essential. Automation plays a pivotal role in reducing response times, as it enables the rapid containment of potential threats. Automated playbooks can be triggered during incidents, ensuring a standardized, swift, and efficient response that minimizes potential damage.

Cybersecurity Workforce Trends and Industry Needs

The BFSI industry faces a talent shortage in the cybersecurity domain, reflecting broader industry trends. According to research, the global cybersecurity workforce needs to grow by 3.4 million to meet the current demand.

BFSI companies must prioritize attracting, developing, and retaining cybersecurity talent, with an emphasis on training professionals to handle both emerging technologies and sophisticated attack methods.

Upskilling current IT staff with cybersecurity knowledge is a vital strategy, as is investing in certifications and partnerships with educational institutions to create a pipeline of future talent.



Best Practices for an Integrated Cybersecurity Approach

1. **Comprehensive Risk Assessment:** Regularly evaluate risks across all operational areas to identify potential vulnerabilities.
2. **Security Awareness Training:** Educate employees about security best practices and foster a culture of vigilance towards cyber threats.
3. **Adopt Zero Trust Architecture:** Implement a Zero Trust model to ensure that all users, both inside and outside of the network, are authenticated and continuously verified.
4. **Utilize Multi-Factor Authentication (MFA):** Strengthen access controls to critical systems and data by employing MFA.
5. **Regulatory Compliance:** Stay abreast of regulatory changes and ensure that security protocols align with industry standards.
6. **Data Encryption:** Encrypt sensitive data both at rest and in transit to protect against unauthorized access.
7. **Incident Response and Disaster Recovery:** Develop and routinely update incident response and disaster recovery plans to ensure preparedness for potential breaches. Also, in case of a security incident, take help of managed security providers like Cyble.

Cyble not only provides a comprehensive Digital Forensics and Incident Response (DFIR) services to help businesses effectively manage, mitigate, and recover from cybersecurity incidents but also ensures that your organization is protected, prepared, and resilient in the face of next-gen cyber threats.

Conclusion

An integrated approach to cybersecurity is crucial for the BFSI industry to safeguard sensitive data, maintain customer trust, and comply with regulatory requirements. By enhancing SOC capabilities, leveraging advanced technologies, and adopting comprehensive security practices, organizations can achieve resilience against adversaries, thereby protecting both their operations and their brand reputation.

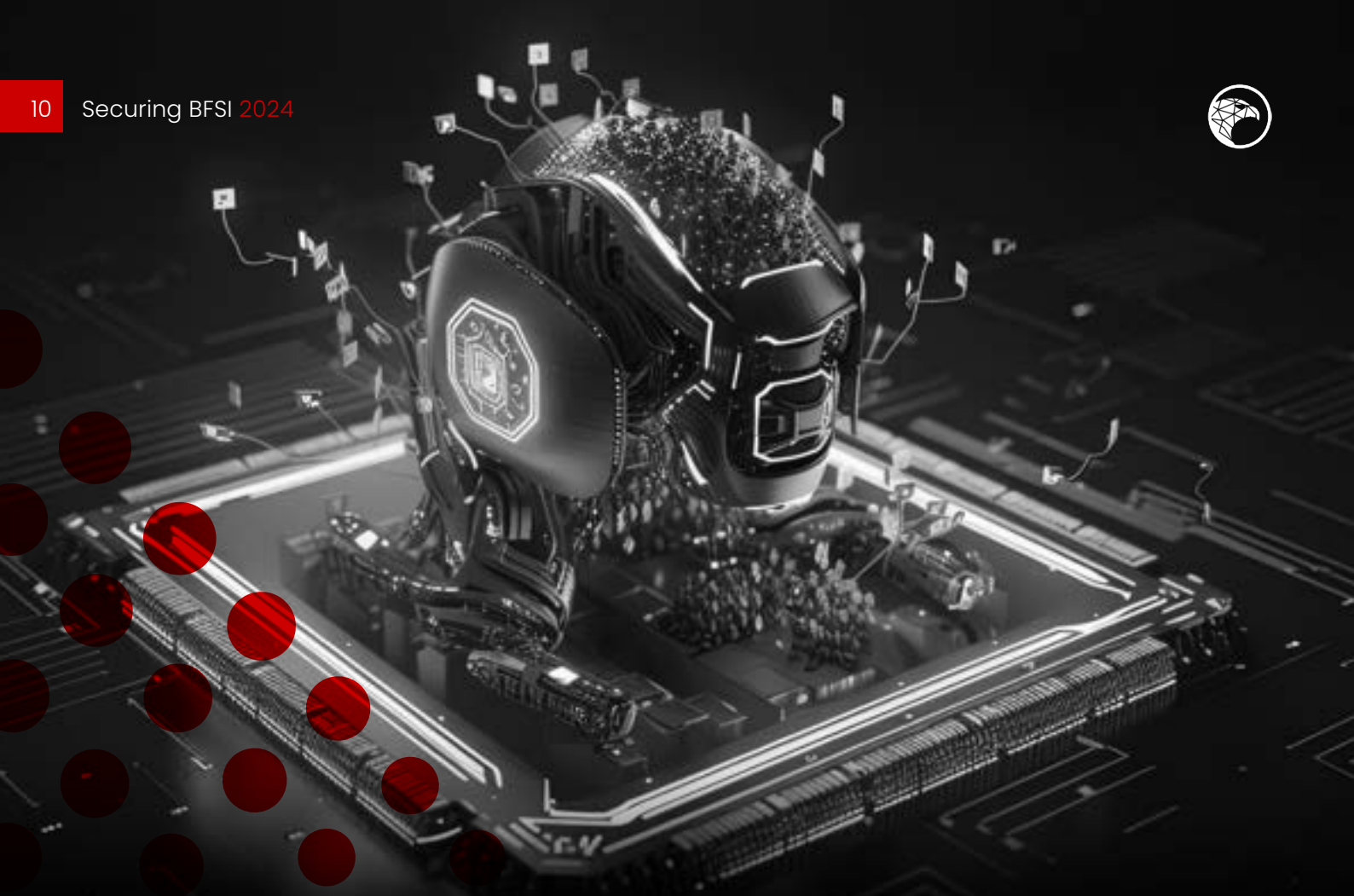
As a leading AI-powered cyber threat intelligence company, we at Cyble understand the ever-evolving threat landscape in the BFSI sector and the need for proactive measures to secure critical assets. With cyberattacks growing in frequency and sophistication, your business can't afford to wait.

Act now to safeguard your financial infrastructure!

Leverage our cutting-edge threat intelligence solutions to stay ahead of attackers. From advanced ransomware detection to AI-powered anomaly tracking, we provide you with real-time insights to secure your organization and protect your brand.

Let's strengthen your defenses together!

Contact us today for a consultation and ensure your BFSI institution is equipped to tackle tomorrow's cyber threats.



About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067