International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

A Review on the Benefits of Continuous Threat Exposure Management in the Banking Industry

Deepa Ajish
IT Security & Compliance, ServiceNow Automation, Los Angeles, California, USA

ABSTRACT: The digital infrastructure of any organization, especially in the banking and financial services sector, is a critical component that underpins its operations. Managing the security of this digital landscape is a formidable challenge, given the ever-evolving threat landscape and the myriad entry points that cyber adversaries can exploit. Continuous threat exposure management offers a proactive approach to identifying, assessing, and managing security threats and vulnerabilities within an organization's IT infrastructure. This review aims to analyze the various benefits associated with continuous threat exposure management, such as proactive risk identification, threat prioritization, and risk resilience strategies. By examining these key areas, this review provides valuable insights into the importance of effectively managing and mitigating threats for the long-term stability and security of financial institutions.

KEYWORDS: Banking, Continuous threat exposure management, CTEM, Cybersecurity, Risk management

INTRODUCTION

The digital revolution has brought about significant changes in the banking industry, with online transactions and digital banking becoming the norm. However, this shift has also opened up new avenues for cyber threats, making cybersecurity a critical concern for the banking industry. This scholarly article delves into the benefits of continuous threat exposure management (CTEM) in fortifying cybersecurity within the banking and financial sector.

In the evolving landscape of the digital economy, the importance of cybersecurity in the banking sector is escalating [1]. The banking and financial industry, where substantial monetary assets are at stake, faces a heightened risk of significant disruption if their systems are compromised [2]. The potential for considerable economic turmoil underscores the gravity of these threats. Thus, the need for robust cybersecurity measures in the banking industry is not just a matter of protecting financial assets but also of preventing large-scale economic instability [2].

In the realm of banking, the incidence and complexity of cyber-attacks have seen a marked increase. From 2018 to 2022, the Federal Bureau of Investigation (FBI) recorded 3.26 million complaints pertaining to cyber-attacks, culminating in reported losses amounting to $27.6 billion [3]. Since financial institutions are the primary attack targets, investments in protection continue to scale. The market value reached $38.72 billion in 2021, and projections see a compound growth rate of 22.4% and a value of $195.5 billion by 2029 [4]. The scope of these attacks is extensive, spanning from intrusions on web-based services to tactics aimed at the transaction systems directly. Organized factions and internal actors are exploiting advanced technologies, such as machine learning, to illicitly access banking resources.

The adoption of cloud computing in the banking sector has been a topic of significant interest in recent years. Cloud computing offers numerous benefits to banks, including improved data processing speed, reduced infrastructure costs, and simplified configuration and security [5]. It also provides a dependable, scalable, and flexible data system that enables traditional banks to modernize quickly and stay abreast of the innovations that 'born-in-the-cloud' challenger banks are bringing to the market [6].

However, the adoption of cloud computing in banking has not been without challenges. Concerns about costs, security, latency, and other factors have led to roadblocks in the path to cloud adoption [7]. The banking sector has exhibited a comparatively measured pace in the adoption of cloud computing, lagging behind other industries. This cautious approach is primarily driven by apprehensions surrounding potential cybersecurity vulnerabilities inherent in cloud technologies, and the ability of cloud service providers (CSP) to adhere to the intricate regulatory framework that rigorously oversees the industry. The integration of cloud computing introduces an additional layer of risk due to the frequent outsourcing of critical services to third-party providers. This outsourcing complicates efforts to uphold data security and privacy, ensure continuous data and service availability, and demonstrate

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

compliance with relevant regulations. This highlights the critical interplay between technological advancement, regulatory compliance, and cybersecurity in the banking industry's digital transformation journey.

Despite these challenges, the trend towards cloud adoption in banking is accelerating. The need for superior speed and agility continues to push banking and financial organizations toward cloud adoption [7]. Furthermore, the advent of hybrid and multi-cloud approaches is expanding the possibilities for how banks can leverage cloud [6, 8].

According to research done by Mordor Intelligence, the market for cloud security solutions in the banking sector is set to grow at a CAGR of 33.1% for the forecast period (2021 - 2026) [9]. The financial industry is a prime target for cybercriminals due to its high volume of valuable financial data and assets [10]. Cybersecurity is critical to the financial industry's success, protecting sensitive customer data, ensuring the integrity of financial transactions, and confirming compliance with regulatory requirements [10].

The banking industry is witnessing a significant digital transformation, with cloud computing playing a pivotal role. As the banking industry continues to adapt to the digital age, the importance of robust cybersecurity measures, including CTEM cannot be overstated. Banks must continually update their cybersecurity strategies to protect against evolving threats and ensure the secure and efficient operation of their services.

A. Cloud Computing

Cloud computing is a form of computing where networks, data storage, applications, security, and development tools are all enabled via the Internet [11]. The inception of cloud computing, a technology for managing virtual data resources, can be traced back to the 1960s. However, it wasn't until the dawn of the 21st century that it gained widespread recognition. This surge in popularity was initiated by the launch of Amazon Web Services in 2006. This was closely followed by the introduction of IBM's enterprise cloud solutions in 2007, Google's App Engine in 2008, Alibaba Cloud in 2009, and Microsoft's Azure in 2010 [12].

The primary categories of cloud computing models are:

1) **Infrastructure as a Service (IaaS):** IaaS is a form of cloud computing that provides virtualized computing resources over the internet [13]. IaaS delivers cloud computing infrastructure including servers, network, operating systems, and storage, through virtualization technology [14].
2) **Platform as a Service (PaaS):** PaaS is a type of cloud computing service that offers a platform for customers to create, operate, and manage applications [13]. This is done without the need for the intricate process of building and maintaining the infrastructure that is usually required for application development and deployment [14].
3) **Software as a Service (SaaS):** SaaS is a model of cloud computing that delivers software applications over the internet on a subscription basis [15]. The service provider manages the hardware and software, and with the appropriate service agreement, will ensure the availability and security of the app and your data [15].

B. Continuous Threat Exposure Management (CTEM)

CTEM is a modern security management process that was introduced by Gartner [16]. Its development can be traced back to the need for more proactive and continuous security measures, as opposed to the reactive approaches of traditional cybersecurity.

The traditional way of managing vulnerabilities can be seen as a reactive approach where remedies are applied after a threat has been detected [17]. Assessing security risks was not a continuous process — it was something that was assessed periodically [17]. However, in today's digital landscape where every attack surface is evolving non-stop, such reactive vulnerability management does not adequately reduce an organization's exposure to vulnerabilities [17].

CTEM, on the other hand, focuses on identifying threats before they can be exploited by continuously monitoring and assessing for vulnerabilities [17]. This enables organizations to respond to security risks faster than previous approaches. Thus, CTEM is a proactive and continuous approach [17]. CTEM is a crucial cybersecurity process that aims to proactively identify and mitigate threats to an organization's networks and systems. Unlike episodic approaches that react to specific incidents, CTEM focuses on ongoing vigilance and risk reduction [18].

Understanding CTEM - The CTEM cycle comprises five stages:

1) **Scope Assessment:** CTEM begins by defining the organization's attack surface—the vulnerable entry points and assets that extend beyond traditional vulnerability management programs. This scope includes not only devices and applications

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

but also less tangible elements like corporate social media accounts, online code repositories, and integrated supply chain systems. Two key areas for initial CTEM initiatives are:

- External Attack Surface: This area combines a relatively narrow scope with a growing ecosystem of tools.
- SaaS Security Posture: Given the rise of remote work, assessing SaaS security has become increasingly important.

2) **Asset Discovery and Risk Profiling:** The discovery process identifies both visible and hidden assets, vulnerabilities, misconfigurations, and other risks. It's essential to differentiate between scoping and discovery—success lies in accurately scoping based on business risk and potential impact.
3) **Threat Prioritization:** CTEM doesn't aim to fix every security issue; instead, it prioritizes threats most likely to be exploited. Factors considered during prioritization include:
   - Urgency
   - Security availability of compensating controls
   - Tolerance for residual attack surface
   - Level of risk posed to the organization

   The focus should be on high-value assets and a treatment plan tailored to address them effectively.
4) **Attack Simulation and Response Evaluation:** CTEM involves simulating attacks to validate vulnerabilities and assess system reactions. Key considerations include:
   - Confirming exploitable vulnerabilities: Ensuring attackers can exploit identified vulnerabilities.
   - Analyzing attack pathways: Identifying potential routes to high-value assets.
   - Response plan evaluation: Assessing the effectiveness and speed of existing response plans.

5) **Mobilization:** This step aims to align everyone within the organization, remove obstacles, and ensure practical implementation. It's not about deploying complex automated systems that magically fix security issues. Instead, the focus is on creating a streamlined and well-defined process. Organizations must ensure that all teams are on the same page regarding security risks. Clear communication and shared understanding are essential. The goal is to empower teams to take action based on what they've learned about security risks. This should be straightforward and hassle-free. Security automation should seamlessly integrate with existing organizational processes. It's about enhancing efficiency, not creating additional complexity. Security efforts and risk management plans must align with the broader business goals. Security should not be an isolated function; it contributes to overall organizational success.

CTEM provides a proactive and dynamic approach to cybersecurity, enabling organizations to stay ahead of threats and protect critical assets effectively [18-20]. Researchers and practitioners alike recognize its significance in an ever-evolving threat landscape.

LITERATURE REVIEW

Banks play a pivotal role in the global economy, handling vast amounts of sensitive information and facilitating transactions. Nevertheless, their dependence on technology, cloud computing, and external vendors renders them vulnerable to cybersecurity risks, including data breaches, ransomware incidents, and identity theft. Reference [21] says that the banking industry has been a major target of cyberattacks due to the critical data that it contains. In 2022, financial institutions ranked as the second most affected sector in terms of reported data breaches [22]. Among the countries impacted by data breaches, the United States, Argentina, Brazil, and China stood out as the most affected [22]. By December 2022, global finance and insurance organizations collectively experienced 566 breaches, leading to the exposure of over 254 million leaked records [22].

Notably, ransomware attacks targeting financial services have surged. In 2023, these attacks increased from 55% (reported in 2022) to 64%, nearly doubling the 34% reported in 2021. Alarmingly, only 1 in 10 attacks were thwarted before encryption occurred, leaving a staggering 81% of organizations falling victim to data encryption [22].

The financial sector bears substantial costs due to data breaches, ranking second highest among all industries, with an average cost of $5.9 million per breach [22].

In 2016, over 3.4 billion individuals accessed the internet. Projections indicate that by 2025, this number will exceed 5 billion, representing a substantial 30% increase within a decade [23]. Research indicates that the expansion of digitalization and connectivity

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

will continue to grow in the coming years due to the increased efficiencies resulting from big data analysis, cognitive systems, and cloud computing [23]. As digitalization continues to expand, the cyber threat against financial institutions grows more pronounced. It's not merely the quantity of cyber-attacks that is on the rise; their intensity, sophistication, and organization are also escalating [24].

As cybersecurity risk has appeared as a significant threat to the financial sector, researchers and analysts are trying to understand this problem from different perspectives [25]. The surge in technology adoption has revolutionized our world, offering efficiency, scalability, and convenience. However, this digital transformation has a darker side—escalating cybersecurity risks. While technology itself remains neutral, it is the human factor that shapes the landscape of breaches [26].

The estimation of risks often involves considering threats and vulnerabilities [27]. A threat is characterized as "any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the nation through an information system." These adverse impacts can occur via unauthorized access, destruction, disclosure, modification of information, or denial of service [28].

On the other hand, a vulnerability is described as a "weakness in an information system, system security procedures, internal controls, or implementation." Such weaknesses can be exploited or triggered by a threat source. Essentially, vulnerabilities create opportunities for threats to manifest [28].

Organizations employ risk management frameworks to customize risk management best practices according to their specific sector and organizational characteristics [29 - 31]. These frameworks serve as structured sets of management goals and guidelines, facilitating interactions with information security, privacy, and risk. By utilizing risk management frameworks, organizations can strike a balance between risk mitigation and tolerance, safeguard assets, proactively address disruptions, and protect their reputation [29 - 31].

A study by Holzmann and Huppertz [32] suggests that, while regulations significantly contribute to fostering stability within the banking sector, it is essential for financial institutions to go beyond regulatory compliance and proactively recognize and manage potential risks. By taking these proactive measures, banks can strengthen their resilience and reduce the probability and severity of financial crises [32].

Research by Mizrak [33] emphasizes the significance of cultivating a strategic perspective regarding cybersecurity. This involves adopting a proactive stance that incorporates risk management initiatives into the overall organizational strategy [33]. Kedarya and Elalouf [34] say that in the heightening intricacy of the context, adaptability, proactive preventive measures, and swift adjustment to emerging technological and other challenges assume paramount significance for financial institutions [34]. The incorporation of proactive threat intelligence, continuous monitoring mechanisms, and a precisely defined incident response plan are fundamental elements within a robust cybersecurity strategy, argues Dawodu [35].

Despite CTEM's importance in the financial industry, there appears to be a lack of extensive research conducted in this area. A few notable works include Gartner's report on how to manage cybersecurity threats [18], and Stefanini's article on the basics of CTEM [36]. These works provide valuable insights into the concept and implementation of CTEM, but they do not delve into empirical studies or provide comprehensive theoretical frameworks.

The current body of literature primarily focuses on the practical application of CTEM, with less emphasis on theoretical underpinnings or empirical validation. There is a need for more rigorous academic research to validate the effectiveness of CTEM and to develop a comprehensive theoretical framework that can guide its implementation. Moreover, most of the existing literature on CTEM is from industry sources [18, 36], with limited input from academia. This highlights the need for more academic research to provide a balanced perspective and to contribute to the development of CTEM as a field of study.

METHODOLOGY

This study aims to explore the advantages of CTEM in the financial sector and other related industries. To fulfill this aim, a SLR was carried out. The SLR was designed to pinpoint the primary areas of interest within the field. The SLR initiated the formulation of a review protocol, which defined the research goals and the standards for literature inclusion and exclusion. A methodical search strategy was then implemented and it provided a complete summary of the research subject. The discovered studies were assessed for quality, and pertinent data was gathered. This data was subsequently examined and synthesized to address the research question concerning the advantages of CTEM in the financial sector.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

In conclusion, the SLR offered valuable insights into the field and identified areas for future research. The meticulous and systematic methodology of the SLR ensured the reliability and comprehensiveness of this research, making it a significant resource for subsequent studies in this area.

A. Data Collection

To guarantee the relevance and thoroughness of the gathered data, a methodical and focused strategy was employed for the data collection process. A search of the databases was conducted using particular keywords such as "continuous threat exposure management", "CTEM", "Banking", "Bank", and "Risk management". These keywords were combined with the logical operators 'AND' and 'OR' to refine the search outcomes. Specifically, the search string was structured as follows: "continuous threat exposure management" AND "Banking" OR "Bank" AND "Risk management". This search string was intended to fetch articles that discuss the advantages of CTEM in banking sectors. The search was not confined to the body of the articles but also encompassed the article titles and keywords. This ensured a broad coverage of pertinent literature, capturing articles where the primary focus was on the selected topic.

B. Data Processing

Given the nature of the data extraction process, it was acknowledged that the retrieved data might encompass impurities, and not all data procured using the designated keywords would be pertinent to the research aims. To counteract this, a manual categorization process was instituted after extraction. This entailed a thorough examination of the retrieved data to pinpoint and discard any irrelevant or impure data. The categorization process ensured that only data relevant to the research was preserved for subsequent analysis.

BENEFITS OF CTEM IN THE FINANCIAL INDUSTRIES

CTEM provides a systematic approach that enables organizations to efficiently prioritize potential threats and corresponding remediation efforts. This becomes especially crucial in the context of a rapidly expanding attack surface. By adopting the CTEM program, organizations can take proactive steps to address their security risks, staying ahead of evolving threats. Unlike traditional, reactive vulnerability management, the CTEM approach offers a practical and pragmatic strategy for prioritizing and mitigating the most critical risks. Through the ongoing surveillance and evaluation of potential weaknesses, organizations can react to security threats more swiftly than with prior methods. Traditional procedures, while encompassing all sectors or digital assets of an organization, frequently fail to provide an in-depth analysis of numerous focal points. In contrast, CTEM concentrates on the organization's entire attack surface, conducting thorough evaluations. Given the rapid pace of digital transformation and cloud computing, it is increasingly challenging for traditional methods to adapt and prioritize threats. Their effectiveness in countering escalating cyber threats is diminishing. CTEM offers a more methodical and pragmatic approach to the continuous enhancement of priorities. Table I presents a comparative analysis between the CTEM methodology and the traditional approach.

Table I: Comparison of CTEM and traditional approach.

CTEM Model	Traditional Approach
Proactive: Actively surveys for potential weaknesses and threats to avert attacks prior to their occurrence.	Reactive: Depends on vulnerability evaluations at specific moments and responds to identified threats.
Holistic: Adopts a comprehensive perspective of the entire attack surface, which includes networks, applications, devices, physical infrastructure, and even extends to third-party vendors.	Siloed: Typically concentrates on particular domains such as network security or application security, which can result in overlooked areas.
Ongoing enhancements: Advocates for perpetual advancement through consistent assessment, modification, and augmentation, grounded in newly acquired information and insights gained from past experiences.	Fixed state: Perceives security as a static condition, which could potentially neglect the emergence of new threats and vulnerabilities.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

Risk prioritization: Ranks vulnerabilities according to their potential consequences and exploitability, directing resources toward the most severe risks.	Equal protection: The equal protection of all assets is emphasized, a practice that requires more resources and may lack efficiency
Automated: Employs automation for functions such as data gathering, vulnerability detection, and response measures, thereby enhancing both efficiency and efficacy.	Manual: Predominantly dependent on manual operations, which often results in delayed reaction times and the possibility of human-induced errors.
External threat intelligence: Incorporates feeds of external threat intelligence to maintain current awareness of the most recent attack techniques and newly surfacing threats.	Internal knowledge: Dependent on internal knowledge and confined threat intelligence.
Continuous monitoring: Persistently surveils for threats and vulnerabilities, offering instantaneous insights and expedited response times.	Periodic scans: Dependent on intermittent scans and evaluations, resulting in monitoring lapses between these scans.
Collaborative: Takes a unified approach, requiring collaboration across all departments.	Team Focused: Focused on security within discrete teams, which could potentially result in disjointed endeavors.
Critical patch deployment: Focuses on the deployment of patches to address the most critical vulnerabilities first.	Severity based patch deployment: Patch prioritization is based on severity leading to delays in critical patches.
Risk metrics-based reporting: Offers a holistic perspective on the security status of the organization through the use of risk metrics.	Vulnerability-based reporting: Vulnerabilities are assessed based on their quantity and severity.

I give below the key benefits of CTEM in the financial industries:

A. **Proactive Risk Management:** CTEM programs empower organizations to proactively tackle vulnerabilities and threats by continuously scanning and monitoring their digital infrastructure. This comprehensive cybersecurity approach shifts the emphasis from reactive responses to proactive measures, resulting in a stronger defense against cyber threats. Table II provides a comparison of proactive risk management and traditional reactive risk management.

Table II: Comparison of proactive risk management and reactive risk management

Proactive Risk Management	**Reactive Risk Management**
Robust risk culture and effective governance structures.	Focused on regulatory compliance.
Data analytics and advanced technology to prioritize threats.	Historical incident-based approach.
Automated preventive controls.	Reactive risk management relies exclusively on analyzing past incidents and formulating responses based on those incidents.
Simulations and strategic planning to evaluate the potential impact of risks.	Hasty decision-making.
Continuous risk assessment and process improvements.	Static and periodic assessment.
Mitigates the likelihood of future incidents by delineating activity boundaries, where a breach of these boundaries could result in an incident.	Aims to prevent the recurrence of the same or similar incidents that have occurred in the past.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

B. **Threat Prioritization:** CTEM programs empower financial institutions to systematically assess and prioritize threats. The process involves evaluating each threat based on two critical factors:

- Potential Impact on Business: Understanding how a threat could affect business operations, financial stability, reputation, and customer trust.
- Likelihood of Occurrence: Estimating the probability of a threat materializing.

By combining these factors, organizations can rank threats in order of severity. Armed with a prioritized threat list, organizations can allocate resources more effectively. Instead of spreading resources thinly across all threats, they can focus on addressing the most critical risks. This strategic allocation ensures that efforts are concentrated where they matter most. A strategic approach to threat management allows for quicker responses. Table III shows the difference between threat prioritization in the CTEM model and the traditional approach.

Table III: Threat Prioritization Comparison

Threat Prioritization - CTEM	Traditional Approach
Proactively identifies and mitigates potential threats	Focused on addressing existing vulnerabilities
Threat prioritization based on potential impact on the business.	Threat severity based on a common vulnerability scoring system.
Context-aware prioritization approach based on real-world risk factors.	Scores may not accurately reflect the real-world risk to a specific business.
Integration with threat intelligence enhances the accuracy of vulnerability detection and prioritization.	Manual triage.
Focus on the potential impact on the business and address the most critical risks.	Remediation of low-risk vulnerabilities and high-risk ones may remain unaddressed.

C. **Cyber Resilience:** CTEM is not a one-time process; it encourages organizations to iterate and refine their defenses continuously. Regular reassessment ensures that security measures remain relevant and effective. Organizations learn from each assessment cycle. Insights gained from previous evaluations inform adjustments to defenses. Adaptation occurs based on real-world experiences and emerging threat patterns. Over time, this iterative refinement leads to enhanced cyber resilience. Resilience refers to an organization's ability to withstand, adapt to, and recover from cyber incidents. By staying current and adaptive, organizations can better withstand attacks and minimize impact. Table IV compares the CTEM model of cyber resilience with the traditional model.

Table IV: Cyber resilience comparison

CTEM – Cyber Resilience	Traditional Approach
Deeply assesses the entire attack surface of an organization, including areas beyond Common vulnerabilities and exposures (CVEs).	The traditional approaches are based on prioritizing vulnerabilities based on CVEs.
Adopts a proactive stance by continuously monitoring the threat landscape.	Security risks are assessed periodically rather than continuously.
The entire attack surface is assessed including misconfigurations, exposed information, and other threats.	These approaches often lack a deep assessment of various focus areas within an organization.
CTEM prioritizes the remediation of identified threats and vulnerabilities to improve an organization's security posture.	Comprehensively addresses all digital assets, but may not sufficiently mitigate an organization's vulnerability exposure.

D. **Actionable Insights:** CTEM programs extract practical insights from real-time threat data. These insights serve as a foundation for implementing effective remediation strategies. By adopting a data-driven approach, CTEM ensures that decisions are

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

informed by the most up-to-date threat intelligence. Consequently, organizations can execute targeted and impactful remediation efforts.

E. **Alignment with Business Objectives:** A well-implemented CTEM program ensures that cybersecurity strategies are closely aligned with the organization's overall business goals. By understanding these strategic objectives, organizations can tailor their security efforts accordingly. Incorporating business goals into the CTEM program ensures that security efforts are not isolated but actively contribute to organizational success. Rather than hindering business operations, cybersecurity becomes an enabler. When cybersecurity aligns with business objectives, its value increases significantly. It becomes an integral part of achieving organizational milestones and growth.

F. **Adaptability:** In the dynamic landscape of technology and evolving cyber threats, a CTEM program remains adaptable. This adaptability ensures that organizations maintain continuous and relevant protection. Given the rapid emergence of new threats in today's fast-paced digital environment, this flexibility is crucial for effective cybersecurity.

G. **Cost Savings:** Security breaches and related issues can result in various costs, including expenses for recovery, regulatory compliance, and reputational damage. However, CTEM significantly reduces these costs by proactively identifying and mitigating security breaches before they escalate.

A well-implemented CTEM program ensures that the exposure management efforts yield actionable results across various teams within the security and IT organizations. Rather than restricting to inventorying and processing data from disparate vulnerability assessment tools, focus on designing a comprehensive program that manages a broader range of exposures. To foster cross-team collaboration, integrate your CTEM plan with organizational-level remediation and incident workflows. This approach goes beyond automated technical fixes and ensures a holistic approach to security.

An ideal CTEM solution would adopt an asset-centric approach. This encompasses the following aspects:

- **Asset Prioritization:** Each asset (such as servers, applications, or network devices) would be assigned a prioritization score relative to all other assets. This score reflects the asset's criticality, business impact, and vulnerability exposure.
- **Issue Tracking per Asset:** For each asset, a detailed list of issues affecting it would be maintained. These issues could include vulnerabilities, misconfigurations, or other security concerns.
- **Unified CTEM Solution:** By focusing on assets as the foundation, organizations can create a comprehensive master list of issues. This list provides clarity on which specific issues, associated with which assets, require immediate attention.

Table V shows how the asset-centric CTEM model differs from the traditional model.

Table V: Comparison of asset-centric CTEM model and risk-based traditional model.

Asset-centric CTEM Model	Risk-based Traditional Model
Asset prioritization: Each asset is assigned a prioritization score relative to other assets based on factors like vulnerabilities, geopolitical context, industry-specific threats, proof-of-concepts, etc. This score helps determine which assets require immediate attention.	All assets are measured equally: This approach is aimed to provide uniform security measures across all assets within an organization.
Issue tracking: For each asset, a list of specific issues affecting it is maintained. This granular tracking ensures targeted remediation.	Known vulnerabilities: The traditional method is typically based on addressing known vulnerabilities.
Holistic view: CTEM considers the entire ecosystem, not just individual assets.	Lack of comprehensive assessment: It is based on assessing all assets equally and may not deeply assess all assets.
Adaptability: Regular adjustments based on new threats and business needs.	Fixed and periodic: Traditional approaches rely on fixed security measures. Assessment occurs periodically, which may not keep pace with rapidly evolving threats.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

Risk prioritization: Resources are directed towards the most severe risks.	Resource-demanding: Treating all assets equally can be resource-intensive. It requires allocating security resources uniformly across the entire asset landscape.

CTEM not only strengthens the resilience and security of the financial industry but also instills confidence in clients, regulators, and stakeholders, demonstrating a proactive and vigilant approach to safeguarding sensitive information and upholding the trust placed in financial institutions. CTEM plays a pivotal role in the financial industry by providing real-time insight into potential risks and vulnerabilities. This proactive approach allows financial institutions to identify and address security threats before they escalate, ultimately safeguarding sensitive data and maintaining the trust of their clients. By continuously monitoring for threats, financial organizations can stay ahead of emerging cyber threats and ensure the integrity of their operations. Additionally, this ongoing monitoring enables them to comply with regulatory requirements and demonstrate their commitment to maintaining a secure environment for their stakeholders. Moreover, CTEM provides valuable data for risk assessment and trend analysis, enabling financial organizations to make informed decisions about their security investments and strategies. This data-driven approach empowers them to allocate resources effectively and prioritize security measures based on the identified threats and vulnerabilities.

LIMITATIONS

Research into the significance of CTEM in the financial industry, while valuable, is not without its limitations. Here are some potential constraints:

- **Lack of Empirical Data:** Many studies rely on theoretical models and simulations, which may not fully capture the complexities of real-world scenarios. The lack of empirical data can limit the applicability of research findings.
- **Rapidly Evolving Threat Landscape:** The cyber threat landscape is constantly evolving, with new threats and vulnerabilities emerging regularly. This rapid evolution can make it challenging for research to stay current and relevant.
- **Variability in Implementation:** The effectiveness of CTEM can vary greatly depending on how they are implemented within an organization. This variability can make it difficult to draw definitive conclusions about their overall significance.
- **Limited Scope:** Some research may focus on specific aspects of CTEM, potentially overlooking other important factors. This can limit the comprehensiveness of the research.
- **Subjectivity in Risk Assessment:** Risk assessment, a critical component of CTEM, often involves a degree of subjectivity. This can introduce bias and uncertainty into research findings.
- **Regulatory and Compliance Differences:** The regulatory and compliance environment can vary significantly across different regions and sectors within the financial industry. This variability can limit the generalizability of research findings.
- **Reliance on Self-Reported Data:** Some research may rely on self-reported data from organizations, which can be subject to bias and inaccuracies.

These limitations highlight the need for ongoing research and collaboration across academia, industry, and regulatory bodies to enhance the understanding of CTEM's significance in the financial industry. Despite these limitations, the research conducted so far provides valuable insights and contributes to the development of more robust and effective risk management strategies.

CONCLUSION

In conclusion, CTEM provides a proactive, comprehensive, and efficient approach to managing cybersecurity risks, which is crucial in an era of escalating cyber threats. CTEM ensures that the organization's own digital assets are secure and threats are identified and mitigated in real time. This can lead to a more secure and resilient financial industry, capable of protecting sensitive data and maintaining trust in an increasingly digital world. With the industry's heavy reliance on digital technologies and third-party services, coupled with the sensitive nature of financial data, effective risk management is paramount.

While the implementation of CTEM is advantageous, it presents its own set of difficulties. The integration of data from diverse security tools, network infrastructure, and external threat intelligence feeds can be intricate and necessitates expertise. The high volume of alerts produced by continuous monitoring can inundate security teams, necessitating effective filters and prioritization techniques to discern genuine threats. Successful CTEM depends on the sharing of information and collaboration across

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

departments, which can be problematic in organizations with compartmentalized structures. The introduction of new processes and tools can meet resistance from employees who are familiar with traditional security methods. The analysis of vast quantities of data from continuous monitoring demands a robust infrastructure and efficient data processing capabilities. Tools empowered by Artificial Intelligence can assist in managing and processing an excess of data. The adaptation of the CTEM program to perpetually emerging attack techniques and vulnerabilities necessitates continuous monitoring and modifications.

While CTEM is a new and promising approach to managing cybersecurity threats, there is a clear need for more extensive research in this area. Future studies should aim to provide empirical evidence of the effectiveness of CTEM, explore its theoretical foundations, and contribute to the development of best practices for its implementation.

REFERENCES

1. Al-Alawi AI, Al-Bassam MSA (2020) The significance of cybersecurity system in helping managing risk in banking and financial sector. Journal of Xidian University 14:1523–1536. https://doi.org/10.37896/jxu14.7/174
2. Knowledgehut (2024) Cybersecurity in Banking: Importance, Threats, Challenges. https://www.knowledgehut.com/blog/security/cyber-security-in-banking Accessed January 20, 2024
3. Federal Bureau of Investigation (2022) Federal Bureau of Investigation Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf Accessed January 20, 2024
4. Epam (2024) The State of Cybersecurity in Banking 2024. https://anywhere.epam.com/business/cyber-security-in-banking Accessed February 10, 2024
5. Yan G (2017) Application of cloud computing in banking: Advantages and challenges. In: 2017 2nd International Conference on Politics, Economics and Law (ICPEL 2017). Atlantis Press, pp 29–32
6. Finextra (2022) Why cloud adoption is on the rise in banking. https://www.finextra.com/blogposting/21824/why-cloud-adoption-is-on-the-rise-in-banking Accessed February 02, 2024
7. McKinsey (2021) Accelerating hybrid-cloud adoption in banking and securities. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/accelerating-hybrid-cloud-adoption-in-banking-and-securities Accessed February 02, 2024
8. BCG (2021) Financial Institutions Need to Pursue Their Own Path to the Cloud. https://www.bcg.com/publications/2021/strategies-for-financial-institutions-transitioning-to-the-cloud Accessed February 02, 2024
9. Mordor Intelligence (2024) Cloud Security in Banking Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) https://www.mordorintelligence.com/industry-reports/cloud-security-in-banking-industry Accessed February 02, 2024
10. EC-Council University (2023) The Importance of Cybersecurity in the Financial Industry. https://www.eccu.edu/blog/cybersecurity/why-is-cyber-security-important-in-the-financial-industry/ Accessed February 02, 2024
11. Southern New Hampshire University (2022) What is Cloud Computing?. https://www.snhu.edu/about-us/newsroom/stem/what-is-cloud-computing Accessed January 03, 2024
12. Cheng M, Qu Y, Jiang C, Zhao C (2022) Is cloud computing the digital solution to the future of banking? Journal of Financial stability 63:101073. https://doi.org/10.1016/j.jfs.2022.101073
13. Palos-Sanchez PR, Arenas-Marquez FJ, Aguayo-Camacho M (2017) Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. Mobile Information Systems 2017:. https://doi.org/10.1155/2017/2536040
14. Rani D, Ranjan RK (2014) A comparative study of SaaS, PaaS and IaaS in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering 4:
15. Chuang I-H, Li S-H, Huang K-C, Kuo Y-H (2011) An effective privacy protection scheme for cloud computing. In: 13th International Conference on Advanced Communication Technology (ICACT2011). IEEE, pp 260–265
16. Reflectiz (2023) What is CTEM? A Complete Overview. https://www.reflectiz.com/blog/what-is-ctem/ Accessed February 02, 2024

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 07 Issue 04 April 2024
DOI: 10.47191/ijcsrr/V7-i4-21, Impact Factor: 7.943
IJCSRR @ 2024
www.ijcsrr.org

17. Splunk (2024) Continuous Threat Exposure Management (CTEM). https://www.splunk.com/en_us/blog/learn/continuous-threat-exposure-management-ctem.html Accessed February 02, 2024
18. Gartner (2023) How to Manage Cybersecurity Threats, Not Episodes. https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes Accessed February 04, 2024
19. Picus Labs (2023) What Is Continuous Threat Exposure Management (CTEM)?. https://www.picussecurity.com/resource/glossary/what-is-continuous-threat-exposure-management-ctem Accessed February 04, 2024
20. CTI Technology What Is A Continuous Threat Exposure Management System?. https://ctinc.com/what-is-a-continuous-threat-exposure-management-system/ Accessed February 04, 2024
21. Firoozi M, Mohsni S (2023) Cybersecurity disclosure in the banking industry: a comparative study. International Journal of Disclosure and Governance 20:451–477. https://doi.org/10.1057/s41310-023-00190-8
22. SentinelOne (2023) Cyber-attacks on Financial Institutions | Why Banks Are Caught in the Crosshairs. https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/ Accessed February 12, 2024
23. World Ecconomic Forum (2016) Understanding Systemic Cyber Risk. https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf Accessed February 10, 2024
24. Gulyás O, Kiss G (2023) Impact of cyber-attacks on the financial institutions. Procedia Computer Science 219:84–90. https://doi.org/10.1016/j.procs.2023.01.267
25. Uddin MH, Ali MH, Hassan MK (2020) Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management 22:239–309. https://doi.org/10.1057/s41283-020-00063-2
26. Eling M, Wirfs J (2019) What are the actual costs of cyber risk events? European Journal of Operational Research 272:1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021
27. Karabacak B, Tatar Ü (2014) Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection. Critical Infrastructure Protection 116:63
28. FIPS (2006) Minimum security requirements for federal information and information systems. https://csrc.nist.gov/pubs/fips/200/final Accessed February 04, 2024
29. Handfield RB, Bechtel C (2002) The role of trust and relationship structure in improving supply chain responsiveness. Industrial marketing management 31:367–382. https://doi.org/10.1016/S0019-8501(01)00169-9
30. NIST Computer Security Resource Center (2016) NIST Risk Management Framework. https://csrc.nist.gov/Projects/risk-management/about-rmf Accessed February 06, 2024
31. Investopedia (2022) Risk Management Framework (RMF). https://www.investopedia.com/articles/professionals/021915/risk-management-framework-rmf-overview.asp Accessed February 06, 2024
32. Holzmann L, Huppertz J (2023) The collapse of Silicon Valley Bank–The importance of proactive risk management in order to prevent financial contagion. In: Konference doktorandů. p 70
33. Mizrak F (2023) Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management 10:98–108. https://doi.org/10.17261/Pressacademia.2023.1807
34. Kedarya T, Elalouf A (2023) Risk management strategies for the banking sector to cope with the emerging challenges. Foresight and STI Governance (Foresight-Russia till No 3/2015) 17:68–76. https://doi.org/10.17323/2500-2597.2023.3.68.76
35. Dawodu SO, Omotosho A, Akindote OJ, et al (2023) Cybersecurity risk assessment in banking: methodologies and best practices. Computer Science & IT Research Journal 4:220–243. https://doi.org/10.51594/csitrj.v4i3.659
36. Stefanini (2023) The Basics Of Continuous Threat Exposure Management (CTEM). https://stefanini.com/en/insights/news/the-basics-of-continuous-threat-exposure-management-ctem Accessed January 20, 2024

*Cite this Article: **Deepa Ajish** (2024). A Review on the Benefits of Continuous Threat Exposure Management in the Banking Industry. International Journal of Current Science Research and Review, 7(4), 2169-2179*