An Eventful Cybersecurity Year: 2022 in Review

Author

Tina Sarsah

Senior Information Systems, Booz Allen Hamilton, Virginia, USA

DOI: *https://doi.org/10.21590/0c2ftr36*

Abstract

The year 2022 was marked by intense cybersecurity activity, with high-profile data breaches, evolving threat tactics, and expanding digital attack surfaces across sectors. A review by Forbes and multiple industry sources noted heightened nation-state cyber aggression, persistent supply chain vulnerabilities, and complications arising from remote work infrastructures. Concurrently, a global shortage of skilled cybersecurity professionals placed additional strain on security teams. Regulatory pressure increased as new compliance frameworks emerged worldwide, pushing organizations toward accountability and risk transparency. More importantly, 2022 signaled a philosophical shift—from focusing solely on breach prevention to embracing resilience through rapid detection, containment, and recovery. This article provides a comprehensive overview of key incidents, trends, and lessons, urging leaders to prioritize cybersecurity as a core business function rather than a reactive cost center.

Key Words: *Salesforce, SAP ERP, MuleSoft, Middleware Architecture, Data Integration, Platform Events, Real-time Synchronization, Apex, Retail IT, System Interoperability.*

1. Introduction

Cybersecurity in 2022 stood at the intersection of geopolitical tension, technological acceleration, and regulatory evolution. While previous years emphasized perimeter defense and compliance checklists, 2022 revealed the limitations of such approaches. Ransomware attacks disrupted global logistics, state-sponsored cyber operations targeted democratic institutions, and zero-day vulnerabilities caught major vendors off-guard. At the same time, remote work models and cloud adoption continued to widen the attack surface. In this volatile environment, resilience—not perfection—emerged as the new cornerstone of digital defense.

2. High-Profile Breaches and Incident Trends

From private corporations to public institutions, few were spared from cyberattacks in 2022. Key breaches included:

- Uber (September 2022): A teenage hacker reportedly exploited weak internal controls and social engineering to gain access to internal systems, highlighting human factor vulnerabilities.
- Medibank (October 2022): One of Australia's largest health insurers was hit by a ransomware attack, leaking sensitive medical records.

- Costa Rica (April 2022): The Conti ransomware gang paralyzed over 27 government institutions, forcing the country to declare a state of emergency.
- LastPass (August–December 2022): A breach affecting the password manager exposed encrypted vaults and prompted an industry-wide discussion about password storage and encryption standards.

These incidents reflected a broader trend: cybercriminals no longer focused solely on financial gain but expanded into politically motivated disruption, identity theft, and reputational damage.

3. Growing Attack Surfaces and Complexity

3.1 The Remote Work Paradigm

Hybrid and remote work models, solidified by pandemic-era digital transformations, continued to challenge traditional IT security structures. Endpoints beyond enterprise control, insecure home networks, and shadow IT practices introduced inconsistencies that attackers exploited.

3.2 Cloud Adoption and Misconfigurations

Organizations rapidly adopted cloud platforms to support agility and scalability. However, many failed to secure these environments properly. Common issues included:

- Publicly exposed storage buckets
- Misconfigured access control lists (ACLs)
- Lack of identity federation across cloud providers

3.3 Supply Chain Vulnerabilities

Following the 2021 Log4Shell incident, supply chain security remained a top concern in 2022. Threat actors continued targeting open-source packages, code repositories, and third-party software providers, exploiting trust relationships to gain deeper access into enterprise systems.

4. Nation-State Activity and Geopolitical Risk

Cyber operations became deeply intertwined with global conflicts:

- **Ukraine-Russia War:** Cyberattacks accompanied kinetic warfare, including data-wiping malware (HermeticWiper), DDoS campaigns against Ukrainian banks, and misinformation targeting civilians.
- **Iranian and North Korean Activity:** APTs from these nations were linked to espionage against critical infrastructure, including nuclear research, healthcare systems, and financial institutions.
- **China-Based Actors:** Continued efforts to exploit zero-day vulnerabilities in telecom, tech, and government systems underscored persistent cyber espionage threats.

These campaigns blurred the lines between military, civilian, and corporate targets—creating a "gray zone" battlefield in cyberspace.

5. Cybersecurity Talent Shortage

Despite increased spending, many organizations faced operational challenges due to a global shortage of cybersecurity professionals. According to (ISC)², the workforce gap exceeded 3.4 million unfilled roles by the end of 2022.

Consequences included:

- Delayed response to alerts and incidents
- Underutilization of security tools
- Burnout among overextended IT staff

Efforts to bridge this gap included upskilling, certification grants, and workforce development partnerships. However, results remained limited in the short term.

6. Regulatory Momentum and Compliance Frameworks

In 2022, global regulators increased pressure on enterprises to report, mitigate, and prepare for cyber threats:

- **United States:** The SEC proposed new rules requiring public companies to disclose cybersecurity incidents within four days and report risk governance strategies.
- **European Union:** The Digital Operational Resilience Act (DORA) and NIS2 Directive expanded compliance obligations for financial institutions and critical infrastructure operators.
- **Asia-Pacific:** Japan and Singapore advanced national cybersecurity strategies mandating security audits and threat intelligence sharing.

These measures indicated that governments are moving from advisories to enforceable mandates—elevating cybersecurity to a board-level concern.

7. Rise of Cyber Resilience over Prevention

Increasingly sophisticated, fast-moving attacks exposed the limitations of absolute prevention. As a result, the cybersecurity philosophy shifted toward resilience, focusing on:

- **Detection:** Early warning systems through SIEM, EDR, and XDR platforms.
- **Containment:** Segmentation, isolation of infected systems, and kill-switch controls.
- **Recovery:** Immutable backups, cloud failovers, and business continuity plans.

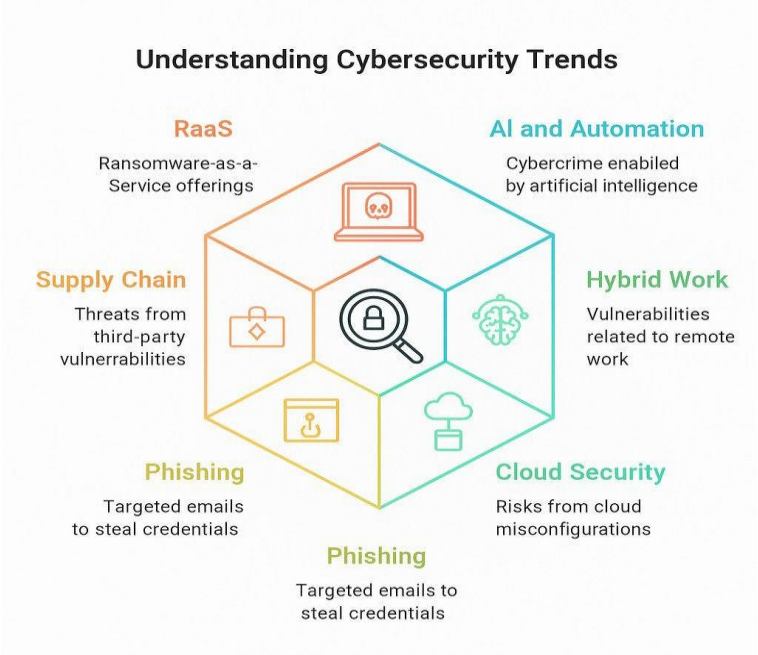
Frameworks like the NIST Cybersecurity Framework and MITRE ATT&CK provided tactical playbooks for resilience-focused operations.

8. Strategic Investments and the Changing Role of CISOs

Security budgets grew in 2022, not only in large enterprises but also in mid-market firms. However, spending patterns shifted:

- More investment in cloud-native security tools (e.g., CNAPP, CSPM)
- Higher allocation for cybersecurity training and simulations
- Growing interest in cyber insurance, despite increased premiums and stricter underwriting

CISOs were increasingly expected to align security with business goals, report directly to the board, and manage third-party risk alongside IT infrastructure.



9. Key Takeaways and 2023 Outlook

2022 Trend	2023 Implication
Nation-state cyber activity	Elevate geopolitical risk analysis within security teams
Cloud misconfigurations	Prioritize multi-cloud governance and posture management
Remote work vulnerabilities	Invest in secure access, device management, and SASE
Regulatory frameworks	Prepare for mandatory breach reporting and audits
Talent shortages	Automate Tier 1 tasks and invest in human capital
Emphasis on resilience	Integrate detection and response across all domains

10. Conclusion

2022 was a turning point for global cybersecurity. It revealed the fragility of overextended IT ecosystems, the growing aggression of state-aligned actors, and the limitations of reactive security models. But it also demonstrated the maturity of resilience thinking, the importance of business-aligned security leadership, and the critical value of regulatory accountability. Going forward, organizations must adopt a proactive, intelligence-driven, and resilience-focused cybersecurity posture—one that treats security as both a strategic investment and a core enabler of business continuity and trust.

References

1. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12
2. Jena, J. (2018). The impact of gdpr on u.S. Businesses: Key considerations for compliance. International Journal of Computer Engineering and Technology, 9(6), 309-319. https://doi.org/10.34218/IJCET_09_06_032
3. Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A review. *American Journal of Science, Engineering and Technology*. https://doi.org/10.22541/au.166385207.73483369/v1
4. Nalluri, S. K., & Parasaram, V. K. B. (2016). Early Approaches to Robotic Process Automation in Enterprise Systems. International Journal of Humanities and Information Technology, 1(01), 12-28. https://doi.org/10.21590/ijhit.01.01.06
5. Parasaram, V. K. B., & Nalluri, S. K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 8(02), 147-155. https://doi.org/10.18090/samriddhi.v8i2.7149
6. Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep reinforcement learning for cybersecurity threat detection and protection: A review. *arXiv preprint*. https://doi.org/10.48550/arXiv.2206.02733
7. Bellamkonda, S. (2022). Zero Trust Architecture Implementation: Strategies, Challenges, and Best Practices. International Journal of Communication Networks and Information Security, 14, 587-591.
8. Alam, S. (2022). Cybersecurity: Past, present and future. *arXiv preprint*. https://doi.org/10.48550/arXiv.2207.01227
9. Vasoya, S., Bhavsar, K., & Patel, N. (2022). A systematic literature review on ransomware attacks. *arXiv preprint*. https://doi.org/10.48550/arXiv.2212.04063
10. Vangavolu, S. V. (2020). Optimizing MongoDB Schemas for High-Performance MEAN Applications. Turkish Journal of Computer and Mathematics Education, 11(03), 3061-3068. https://doi.org/10.61841/turcomat.v11i3.15236
11. Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Burdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2022). The role of machine learning in cybersecurity. *arXiv preprint*. https://doi.org/10.48550/arXiv.2206.09707
12. Mustafa, N. (2022). Cyber security trends for 2022. *BrightTalk Webinar Series*. https://doi.org/10.13140/RG.2.2.30507.92965
13. Goli, V. R. (2015). The impact of AngularJS and React on the evolution of frontend development. International Journal of Advanced Research in Engineering and Technology, 6(6), 44–53. https://doi.org/10.34218/IJARET_06_06_008
14. Tiutiunyk, I., Kuzior, A., & Kelemen, R. (2023). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(1), 220–239. https://doi.org/10.14254/2071-8330.2023/17-1/12
15. Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep reinforcement learning for cybersecurity threat detection and protection: A review. *arXiv preprint*. https://doi.org/10.48550/arXiv.2206.02733
16. Alam, S. (2022). Cybersecurity: Past, present and future. *arXiv preprint*. https://doi.org/10.48550/arXiv.2207.01227
17. Vasoya, S., Bhavsar, K., & Patel, N. (2022). A systematic literature review on ransomware attacks. *arXiv preprint*. https://doi.org/10.48550/arXiv.2212.04063
18. Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Burdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2022). The role of machine learning in cybersecurity. *arXiv preprint*. https://doi.org/10.48550/arXiv.2206.09707
19. Mustafa, N. (2022). Cyber security trends for 2022. *BrightTalk Webinar Series*.

https://doi.org/10.13140/RG.2.2.30507.92965

20. Tiutiunyk, I., Kuzior, A., & Kelemen, R. (2023). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, *17*(1), 220–239. https://doi.org/10.14254/2071-8330.2023/17-1/12
21. Sewak, M., Sahay, S. K., & Rathore, H. (2022). Deep reinforcement learning for cybersecurity threat detection and protection: A review. *arXiv preprint*. https://doi.org/10.48550/arXiv.2206.02733.