RESEARCH ARTICLE

Cybersecurity Trends 2022: Toward a More Secure Future

Vinay Nandamuri
Infra Technology Specialist, Cognizant, Connecticut, USA

Received: 16/08/2022 **Accepted:** 19/11/2022 **Published:** 31/12/2022

Abstract

The year 2022 marked a pivotal moment in the evolution of cybersecurity. As digital transformation accelerated, so did the sophistication and scale of cyber threats. Check Point Research's report, "Cybersecurity Trends 2022: Toward a More Secure Future," highlighted a series of transformative trends—including the rise of Ransomware-as-a-Service (RaaS), the growing use of artificial intelligence by attackers, and a persistent wave of cloud and supply chain attacks. This paper examines these trends in detail, contextualizes their implications, and outlines strategic responses for building a secure digital future. With threat actors operating as businesses and attack surfaces expanding across cloud, IoT, and hybrid networks, the imperative for proactive, layered, and intelligence-driven security has never been clearer.

Journal of Applied Pharmaceutical Sciences and Research, (2022); DOI: 10.31069/japsr.v5i4.06

Introduction

In the face of unprecedented global cyber activity, 2022 stood out as a year of both escalating threats and emerging resilience strategies. Organizations of all sizes faced growing pressure to secure their environments while navigating hybrid work, digital transformation, and regulatory scrutiny. Threat actors evolved their methods, while defenders adopted new technologies and frameworks to keep pace. The Check Point report served as a crucial guidepost for understanding not just the attacks that occurred, but the trajectory of cybersecurity as a strategic discipline.

Methodology

This research draws upon:

- Primary source analysis of the Check Point Cyber Security Report 2022
- Supplementary data from CrowdStrike, Mandiant, Microsoft, and IBM X-Force
- Cross-referencing with MITRE ATT&CK and CISA advisories
- Qualitative synthesis of industry responses, incident case studies, and expert recommendations

Each trend is analyzed for its scope, impact, technical components, and strategic mitigation.

Key Trends from 2022

Ransomware-as-a-Service (RaaS)

Ransomware continued to dominate headlines, with RaaS platforms like LockBit 2.0 and Conti enabling affiliates to deploy attacks at scale. RaaS lowered the entry threshold for cybercriminals, offering:

- Pre-built ransomware kits
- Negotiation portals
- Cryptocurrency laundering services

Notable incidents:

- Costa Rica government suffered a $100M+ loss and declared a national emergency.
- Medibank in Australia refused ransom demands, leading to full data disclosure.

Implications

Traditional perimeter defenses proved inadequate. Organizations needed layered defenses, including endpoint detection and response (EDR), network segmentation, and offsite backups.

Phishing and Social Engineering

Social engineering tactics became more sophisticated, leveraging:

- Deepfake audio
- Business Email Compromise (BEC)
- MFA fatigue attacks (e.g., Uber breach)

These campaigns often bypassed technical controls by exploiting human behavior.

Mitigation

Continuous user awareness training, phishing simulations, and identity-based analytics became critical.

Supply Chain Attacks

Building on the momentum of 2021's SolarWinds and Log4Shell attacks, adversaries targeted open-source dependencies, CI/CD pipelines, and vendor access points.

High-profile Examples

- Okta breach via a third-party support vendor
- Nvidia source code theft affecting downstream firmware

Strategic need

Widespread adoption of Software Bills of Materials (SBOMs), third-party risk assessments, and supply chain segmentation.

Cloud Vulnerabilities and Misconfigurations

Cloud platforms became a central target, especially in multi-cloud and hybrid deployments.

Common flaws

- Misconfigured IAM roles
- Exposed S3 buckets
- Overly permissive Kubernetes clusters

Recommendations

Cloud Security Posture Management (CSPM), automated compliance scanning, and Zero Trust architectures for access control.

Increased Attack Automation and AI Usage

Threat actors adopted automation to:

- Scan for vulnerable targets in real-time
- Evade detection via polymorphic malware
- Launch mass phishing at scale

Emerging countermeasures

- AI-powered threat detection platforms
- Behavior-based analytics
- Threat intelligence correlation engines

Mobile Threats and BYOD Challenges

The widespread use of personal devices introduced challenges:

- Malware-laced mobile apps
- SMS-based phishing (smishing)
- Insecure VPN or hotspot use by remote employees

Mitigation: Unified Endpoint Management (UEM), mobile threat defense, and remote wipe capabilities.

Cybercrime Becomes Corporate

Cybercrime groups now operate like SaaS companies:

- Recruiting on forums
- Offering 24/7 support
- Publishing version updates and roadmaps

Example

Conti's leaked internal documentation revealed HR departments, performance reviews, and revenue sharing.

Implication

Security teams must match this sophistication with structured, proactive, and intelligence-led operations.

Sectoral Impact

Sector	*Primary Risks*	*2022 Impact*
Healthcare	RaaS, phishing, unpatched IoT	Ransomware disrupted surgeries, leaked PHI
Finance	BEC, cloud exploits, credential stuffing	Wire fraud, regulatory fines
Government	Nation-state malware, DDoS	Disrupted services, compromised communications
Retail	Web skimming, account takeovers	Customer trust loss, PCI-DSS violations
Education	Phishing, endpoint attacks	E-learning disruptions, research data theft

Recommendations for a Secure Future

Adopt a Zero Trust Model

- Enforce continuous identity verification
- Micro-segment networks
- Apply least-privilege access everywhere

Integrate AI and Threat Intelligence

- Implement anomaly detection at network and endpoint levels
- Ingest IOCs and TTPs from threat feeds
- Correlate events across SIEM and XDR platforms

Secure the Cloud by Design

- Use infrastructure-as-code scanning tools
- Automate remediation of misconfigurations
- Encrypt all data in motion and at rest

Rethink User Training

- Move from annual compliance training to real-time micro-learning
- Include phishing drills and red-team simulations
- Train executives and board members on cyber risk exposure

Align Security with Business Goals

- Define cybersecurity ROI through uptime, risk reduction, and brand trust
- Elevate CISO reporting to the board level
- Build security into digital transformation projects

Conclusion

The cybersecurity trends of 2022 revealed a fast-evolving threat landscape where attackers leveraged scale, automation, and human weakness to outmaneuver traditional defenses. The good news: many organizations began recognizing cybersecurity as a core business enabler. Success in 2023 and beyond will depend on shifting from static defenses to adaptive, intelligence-driven models that integrate deeply with operations. As cybercrime becomes increasingly professionalized, so too must our defenses—built on visibility, speed, collaboration, and executive alignment.

References

1. Jena, J. (2015). Next-Gen Firewalls Enhancing: Protection against Modern Cyber Threats. International Journal of Multidisciplinary and Scientific Energing Research, 3(4), 2015-2019. https://ijmserh.com/admin/pdf/2015/10/46_Next.pdf
2. Alam, S. (2022). *Cybersecurity: Past, Present and Future*. arXiv. https://arxiv.org/abs/2207.01227
3. Brooks, C. (2022). A boiling cauldron: Cybersecurity trends, threats, and predictions for 2023. *Forbes*. https://www.forbes.com/sites/chuckbrooks/2022/11/23/a-boiling-cauldron-cybersecurity-trends-threats-and-predictions-for-2023/
4. Eling, M., & Schnell, W. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(1), 1–30. https://doi.org/10.1057/s41288-022-00266-6
5. Bellamkonda, S. (2022). Zero Trust Architecture Implementation: Strategies, Challenges, and Best Practices. International Journal of Communication Networks and Information Security, 14, 587-591.
6. Gartner. (2022). 7 top trends in cybersecurity for 2022. *Gartner*. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022
7. ISACA. (2023). An executive view of key cybersecurity trends and challenges in 2023. *ISACA*. https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023
8. Vangavolu, S. V. (2022). Implementing microservices architecture with Node.js and Express in MEAN applications. International Journal of Advanced Research in Engineering and Technology, 13(8), 56–65. https://doi.org/10.34218/IJARET_13_08_007
9. Krypsys. (2022). Cybersecurity trends so far in 2022. *Krypsys*. https://krypsys.com/cyber-security-2/cybersecurity-trends-so-far-in-2022/
10. Matania, E., & Sommer, U. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science*, 75(2), 140–164. https://doi.org/10.1080/00323187.2023.2278499
11. Matania, E., & Yoffe, L. (2022). Some things the giant could learn from the small: Unlearned cyber lessons for the US from Israel. *The Cyber Defense Review*, 7(1), 101–110.
12. Goli, V. R. (2018). Optimizing and Scaling Large-Scale Angular Applications: Performance, Side Effects, Data Flow, and Testing. International Journal of Innovative Research in Science, Engineering and Technology, 7(2), 1181-1184. https://www.ijirset.com/upload/2018/february/1_Optimizing1.pdf
13. Matania, E., Yoffe, L., & Goldstein, T. (2017). Structuring the national cyber defence: In evolution towards a Central Cyber Authority. *Journal of Cyber Policy*, 2(1), 16–25. https://doi.org/10.1080/23738871.2017.1299193
14. Matania, E., Yoffe, L., & Mashkautsan, M. (2016). A three-layer framework for a comprehensive national cyber-security strategy. *Georgetown Journal of International Affairs*, 17(3), 77–84.
15. Matania, E., & Tal-Shir, E. (2020). Continuous terrain remodeling: Gaining the upper hand in cyber defence. *Journal of Cyber Policy*, 5(2), 285–301. https://doi.org/10.1080/23738871.2020.1778761
16. Ozer, M., Kose, Y., Bastug, M., Kucukkaya, G., & Varlioglu, E. R. (2024). The shifting landscape of cybersecurity: The impact of remote work and COVID-19 on data breach trends. arXiv. https://arxiv.org/abs/2402.06650
17. Security Magazine. (2022). Leading cyber risks and trends in 2022. *Security Magazine*. https://www.securitymagazine.com/articles/98695-leading-cyber-risks-and-trends-in-2022
18. Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, 17(2), 221–234. https://doi.org/10.14254/2071-8330.2024/17-2/12

How to cite this article: Nandamuri V. Cybersecurity Trends 2022: Toward a More Secure Future. Journal of Applied Pharmaceutical Sciences and Research. 2022; 5(4): 37-39 Doi : 10.31069/japsr.v5i4.06