A LOOK BACK AT THE THREAT LANDSCAPE 2024

James Ringold
Dave Spehar

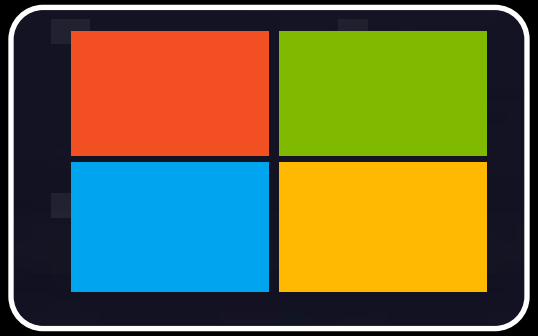
Overview

High rate of internal discovery of security incidents

Impact of the Muddled Libra threat actor

Rise of cloud incidents

Shift towards mass data exfiltration



Convergence of nation-state actors and cybercriminals

Use of cyberattacks in hybrid warfare

Vulnerability of OT systems

Evolution of ransomware

Importance of cloud identity security

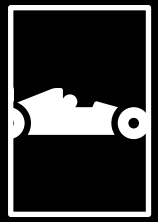
Balance between external and internal detection of compromises

Reduction in dwell time

Industry targeting trends

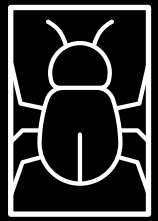
Prevalence of financially motivated attacks

Evolution of malware and phishing techniques.



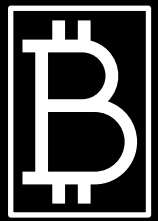
Rapid Attack Progression:

Attackers are moving quickly, often exfiltrating data within hours of initial compromise. This necessitates faster incident response capabilities.



Software Vulnerabilities as Entry Points:

Exploiting software vulnerabilities remains a primary attack vector, highlighting the importance of vulnerability management.



Rise of Extortion:

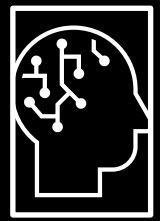
Extortion tactics, including ransomware, are increasingly prevalent and sophisticated.

Muddled Libra's Impact:

The criminal group Muddled Libra is identified as a major threat actor in 2023, known for aggressive tactics and financial motivation.

Incident Discovery Trends:

While internal detection is improving, external notifications are still common, indicating a need for stronger security postures.



AI's Dual Role:

AI is being leveraged by both attackers and defenders, impacting the cybersecurity landscape.

Cloud Incidents on the Rise:

Attacks targeting cloud environments are increasing, requiring enhanced cloud security measures.

Detection Sources:

External notifications are increasingly the primary way organizations learn of compromises, especially in ransomware cases.

Industry Targeting:

Financially motivated attacks are on the rise, with ransomware being a significant driver.

Malware Trends:

While new malware families are being tracked, attackers are also using known tools and exploiting older vulnerabilities.

Cloud Intrusions:

Attackers are targeting cloud environments, requiring adapted security strategies.

Dwell Time:

The global median dwell time has decreased to a record low of 10 days, but regional variations exist.

Threat Techniques:

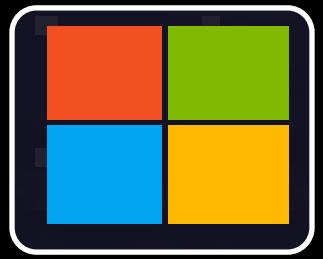
Attackers are focusing on evasion techniques and using zero-day vulnerabilities.

Phishing Evolution:

Phishing remains a threat, with new techniques like smishing and AiTM campaigns bypassing MFA.

Nation-State Activity:

Nation-state actors are using criminal tools and tactics, blurring the lines between espionage and cybercrime.

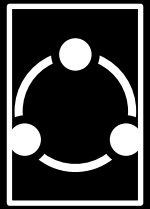


Escalating Cyber Threats:

Attacks from both cybercriminals and nation-state actors are increasing in sophistication and persistence.

Nation-State Threat Activity:

The United States remains a primary target, with other targeted nations experiencing military conflict or geopolitical tensions. Nation-state actors focus on government institutions, critical infrastructure, and research and development industries.



Ransomware Evolution:

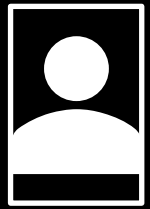
Ransomware attacks are becoming more sophisticated and hybrid, targeting both on-premises and cloud assets. Collaboration between industry, law enforcement, and governments is crucial for disruption efforts.

Microsoft's Secure Future Initiative (SFI):

Microsoft launched this initiative to strengthen its security posture by prioritizing security, mandating phishing-resistant MFA, strengthening corporate network security, expanding security teams, and reducing the attack surface.

Blurring Lines Between Nation-State Actors and Cybercriminals:

Nation-state actors are adopting criminal tools and tactics, making attribution more difficult. They are increasingly involved in financially motivated cybercrime and using criminal infrastructure.



Identity and Social Engineering:

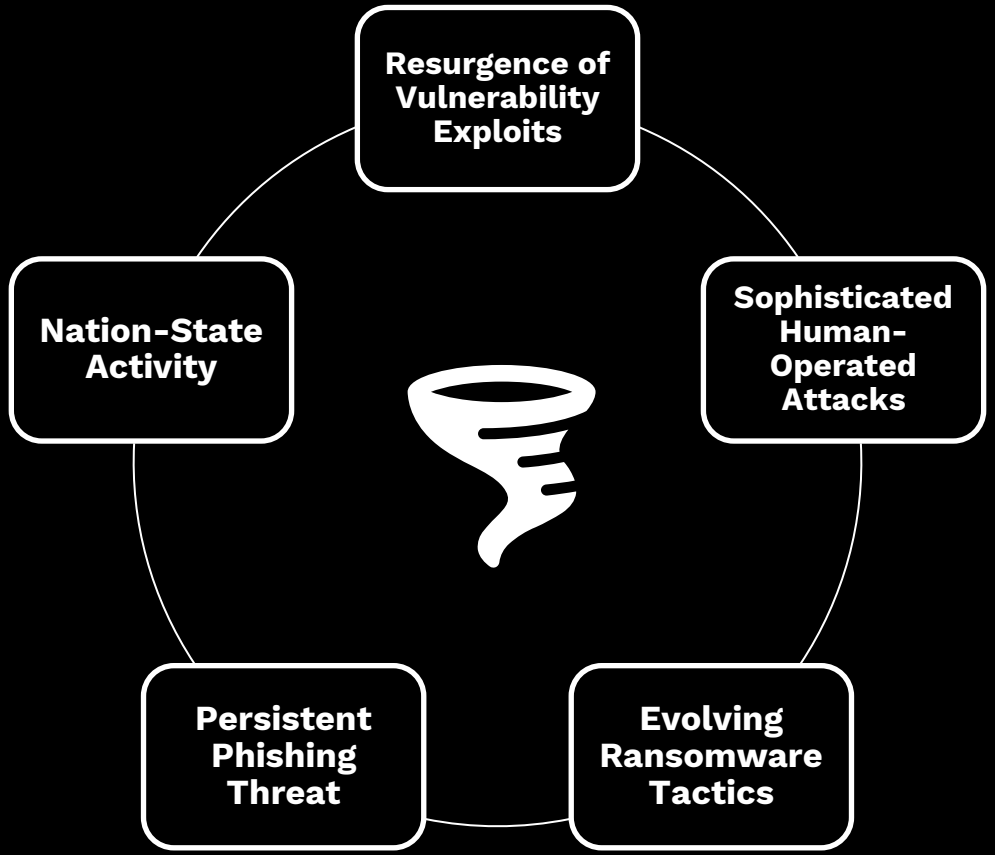
Phishing, password spray attacks, and cloud identity compromise remain major threats.

AI's Impact on Cybersecurity:

AI offers benefits for defense through threat detection, response automation, and streamlined security workflows. However, it also poses risks such as AI-enabled social engineering and AI-powered malware. Global collaboration and policy frameworks are essential to address AI-related security challenges.

Threats

Common Threats Across Cybersecurity Reports



Top Threats Facing Companies

- **Resurgence of Vulnerability Exploits:** Exploiting internet-facing vulnerabilities has surpassed phishing as the primary attack vector. The rise of zero-day exploits, used by both financially motivated actors and espionage groups, is particularly concerning.
- **Sophisticated Human-Operated Attacks:** These attacks go beyond traditional malware infections, employing social engineering, identity compromise, and "living off the land" techniques. Hybrid attacks targeting both on-premises and cloud assets pose a significant challenge.
- **Evolving Ransomware Tactics:** Ransomware continues to evolve, with increased use of data destruction capabilities alongside encryption. Human-operated ransomware attacks are on the rise, and supply chain attacks are being leveraged for wider impact.
- **Persistent Phishing Threat:** Phishing remains a significant risk, with attackers expanding their objectives beyond credential theft and using legitimate services for delivery. User awareness and training are crucial for defense.
- **Nation-State Activity:** Nation-state activity is expanding beyond espionage to include disruptive attacks and influence operations. The lines between state-sponsored actors and cybercriminals are blurring, with financially motivated state-sponsored groups targeting the supply chain.

Consistent Cyber Threats

Highlighted Threats across Cybersecurity Reports

- **Exploitation of Vulnerabilities:** Increased use of exploits, especially zero-days, for initial access. Requires proactive patching and attack surface reduction.
- **Sophisticated Human-Operated Attacks:** Growing challenge of defending against human-driven attacks targeting identity and access. Demands layered security and Zero Trust adoption.
- **Persistent and Evolving Ransomware Threat:** Ransomware remains prevalent, with increased data destruction and hybrid attacks. Strong identity security, backups, and incident response are essential.
- **Phishing: An Enduring Risk:** Phishing persists as a threat, evolving with sophisticated techniques. User awareness, email security, and phishing-resistant authentication are crucial.
- **Blurring Lines: Nation-State Activity and Cybercrime:** Nation-state actors increasingly use criminal tools and tactics. Companies must consider geopolitical factors in risk assessments.

Key Takeaway: The threat landscape is complex and evolving, demanding a proactive, multi-layered, and intelligence-driven approach to cybersecurity.

Defensive Strategies

Key Defensive Strategies - Summarized

Proactive Attack Surface Management	**AI and Automation**	**Zero Trust Network Access (ZTNA)**	**Continuous Monitoring and Incident Simulation**
Threat-Informed Defense	**Robust Identity and Access Management**	**Incident Response Planning and Practice**	**Focus on Evasion Detection**
Defense in Depth	**Prioritized Patching**	**Robust Security Awareness Training**	**Leveraging Red Team Exercises**

Key Defensive Strategies - Unit 42

- **Attack Surface Management:** Proactive management of internet-facing assets is crucial. Regular assessments to identify and prioritize vulnerabilities for remediation are recommended.

- **AI and Automation:** Leveraging AI and automation can modernize security operations, improve response times, and reduce analyst workload. The report recommends Extended Detection and Response (XDR) and Extended Security Intelligence and Automation Management (XSIAM) solutions.

- **Zero Trust Network Access (ZTNA):** Implementing a Zero Trust approach to network security is strongly advocated. ZTNA operates on the principle of "never trust, always verify," requiring continuous authentication and authorization. By enforcing least privilege access and micro-segmentation, ZTNA limits the impact of breaches.

- **Continuous Monitoring and Incident Simulation:** Continuous monitoring across the IT infrastructure is needed for quick threat identification and response. Setting up alerts for suspicious activities (impossible logins, repeated authentication failures, etc.) is recommended. Regular incident simulations, like tabletop exercises and penetration tests, can assess the effectiveness of security controls and response plans.

Key Defensive Strategies - Microsoft Defender

- **Threat-Informed Defense:** This approach shifts from a traditional, checklist-based security approach to a more proactive strategy that focuses on understanding attacker behavior and prioritizing defenses based on the most likely attack paths and critical assets. It involves consolidating threat exposure insights, protecting critical assets, and managing attack paths.

- **Robust Identity and Access Management:** The report stresses the importance of strong identity security, particularly in hybrid and cloud environments. Key recommendations include centralized identity management, multi-factor authentication (MFA) for all users, phishing-resistant authentication methods, and enhanced password reset procedures.

- **Incident Response Planning and Practice:** Microsoft provides guidance on incident response, emphasizing clear communication, well-defined roles, and regular practice of recovery actions. This includes establishing clear reporting lines, detailed incident response plans, alternative communication channels, and regular practice drills.

Key Defensive Strategies - Mandiant

- **Focus on Evasion Detection:** As attackers increasingly employ evasion techniques, organizations must enhance their ability to detect such tactics. This includes monitoring beyond traditional endpoints to encompass critical infrastructure components.
- **Defense in Depth:** A multi-layered security approach is essential to counter sophisticated attackers. Implementing multiple security controls at various levels of the IT infrastructure makes it harder for attackers to breach and navigate within the network.
- **Prioritized Patching:** Patching vulnerabilities should be prioritized based on active exploitation, not just risk scores. Evidence of active exploitation necessitates immediate patching, regardless of the initial risk assessment.
- **Robust Security Awareness Training:** Comprehensive training is crucial to empower employees to identify and avoid phishing attacks, a common entry point for attackers. Training should address evolving phishing tactics.
- **Leveraging Red Team Exercises:** Red team exercises, simulating real-world attacks, can effectively test security controls and incident response capabilities. Mandiant's red and purple teams utilize AI and current attacker tactics to provide valuable insights for organizations.

Comparing Key Defensive Strategies Across Cybersecurity Reports

Convergence:

- **Zero Trust Architecture:** All three reports emphasize Zero Trust as a foundational security model.
- **Identity and Access Management (IAM):** The reports stress the importance of strong IAM, particularly for cloud resources and sensitive data.
- **Speed and Automation:** They advocate for faster and more automated security operations to keep pace with attackers.
- **Security Awareness:** The reports recognize the importance of human awareness and training in cybersecurity.
- **Vulnerability and Exposure Management:** They underscore the ongoing need for robust vulnerability management and patching.

Divergence:

- **Unit 42:** Focuses on incident response and operationalizing security practices.
- **Microsoft:** Emphasizes cloud security, governance, and accountability.
- **Mandiant:** Focuses on threat intelligence, zero-day exploits, and building a comprehensive security program.

Overall: The reports converge on the need for a holistic, proactive, and intelligence-driven approach to cybersecurity.

Key Takeaways:

- **Layered Approach:** Combining Zero Trust, strong IAM, automation, security awareness, and vulnerability management.
- **Proactive Defense:** Shifting from reactive to proactive security measures.
- **Intelligence-Driven:** Utilizing threat intelligence to inform security strategies.

Call to Action

Top 5 Actions for Enhanced Cybersecurity

Implement and Operationalize a Zero Trust Architecture.

Elevate Security to a Shared Organizational Responsibility.

Accelerate Threat Detection and Response with Automation.

Master the Fundamentals: Vulnerability and Exposure Management.

Prepare for the Inevitable: Incident Response Planning and Testing.

Looking Forward

Preparing for the Future: A Call to Action

- **Prioritize a Security-First Culture:** Foster a culture of security awareness and accountability throughout the organization. This involves educating employees about cyber risks, implementing strong security policies, and regularly testing and evaluating security controls.
- **Embrace a Zero Trust Model:** Adopt a Zero Trust approach to network security, where no user or device is implicitly trusted. Implement strong authentication mechanisms, including multi-factor authentication (MFA) and phishing-resistant credentials.
- **Invest in Robust Identity and Access Management:** Prioritize strong identity and access management practices, including least privilege access controls, regular permission reviews, and monitoring for suspicious activity.
- **Proactive Attack Surface Management:** Minimize the attack surface by continuously identifying and mitigating vulnerabilities. Prioritize patching critical vulnerabilities, securing internet-facing assets, and implementing robust endpoint protection.
- **Embrace AI-Powered Security Solutions:** Leverage AI for defense to enhance threat detection, response, and prediction capabilities. Explore AI-powered solutions for threat intelligence, security analytics, and automated incident response.
- **Engage in Collaboration and Information Sharing:** Actively participate in information-sharing initiatives and collaborate with industry peers and security experts to gain valuable insights and resources.

The Darkening Horizon: Challenges on the Cyber Front

- **Sophistication and Scale of Attacks:** The scale and complexity of cyberattacks are expected to increase. Attackers are adopting advanced tools and strategies, including those used by nation-state actors. Organizations must prepare for more complex and damaging attacks that may exceed their current defensive capabilities.
- **Rise of Extortion and Harassment:** The use of extortion and harassment tactics by attackers is on the rise. Organizations need to be prepared for these aggressive tactics and have robust incident response plans in place.
- **Exploitation of AI:** While AI can be leveraged for cybersecurity, attackers can also misuse it to amplify social engineering attacks, create deepfakes, and automate malicious activities. This poses a challenge for defenders.
- **Targeting Beyond the Endpoint:** Attackers are increasingly targeting devices and technologies beyond traditional endpoints, such as edge devices, which often lack robust security solutions. This shift makes visibility and detection more challenging.

Rays of Hope: Opportunities for Strengthening Defense

- **Continued Improvement in Detection and Response:** Despite the increasing sophistication of attacks, defenders are becoming more effective at detecting and responding to threats. The decreasing global median dwell time indicates progress in identifying and mitigating breaches more quickly.

- **Leveraging AI for Defense:** AI presents significant opportunities for enhancing cybersecurity. AI-powered solutions can be used to analyze vast amounts of security data, automate incident response tasks, and even predict and prevent attacks. Organizations can leverage AI to gain a strategic advantage in their defense efforts.

- **Collaboration and Information Sharing:** Collaboration and information sharing within the cybersecurity community are crucial for staying ahead of threats. Sharing threat intelligence, best practices, and lessons learned can help organizations collectively strengthen their defenses and disrupt malicious actors. Initiatives like the Cybercrime Ransomware Initiative (CRI) demonstrate the power of collaboration in combating cybercrime.

Key Statistics

Key Statistics - Mandiant M-Trends

- **Detection Source:** Mandiant's data shows a significant shift in how organizations are detecting cyberattacks. In 2023, more than half (54%) of compromised organizations first learned of a compromise from an external source, up from 32% in 20159. This trend likely reflects the increase in ransomware attacks, where organizations are often notified by the attackers themselves via ransom demands. For non-ransomware intrusions, the split between internal and external discovery was even at 50%.

- **Dwell Time:** Mandiant reports a continued decrease in the global median dwell time, which measures the time between an attacker's initial compromise and their detection. In 2023, the median dwell time was 10 days, down from 16 days in 2022 and a significant improvement from the 416 days reported in 201110. This reduction is attributed to improved detection capabilities and increased awareness of threats. However, Mandiant also observed a rise in intrusions detected after five years or more, suggesting that some attackers remain undetected for extended periods.

- **Financially Motivated Attacks:** The proportion of intrusions serving financially motivated objectives increased to 36% in 2023, up from 26% in 202212. This rise is largely driven by ransomware attacks, which accounted for almost two-thirds of financially motivated intrusions

- **Data Theft:** Mandiant identified data theft in 37% of intrusions in 2023, slightly down from 40% in 202213. In 11% of intrusions, attackers directly monetized stolen data through extortion, and in an additional 7%, they combined data theft with ransomware and extortion. These figures highlight the growing prevalence of data theft as a key objective for attackers and the increasing use of multifaceted extortion tactics.

Key Statistics - Microsoft Digital Defense

- **Scale of Cyberattacks:** Microsoft's network processes a massive 78 trillion security signals daily, highlighting the constant barrage of cyber threats.
- **Nation-State Activity:** Nation-state actors remain active, using cyberattacks to support geopolitical goals, focusing on espionage, disruption, and influence operations.
- **Rise of Cloud Identity Compromise:** Microsoft observes a concerning rise in attacks targeting cloud identities, emphasizing the importance of securing identities in hybrid and cloud environments. They note that only 2.6% of workload identity permissions were actually used, and a concerning 51% of workload identities were completely inactive. This highlights the need for organizations to implement robust identity governance practices to minimize the risk of compromise.
- **Password Spray Attacks:** Password spray attacks remain a persistent threat, with Microsoft's systems defending against 27,860 individual password attacks every second. This staggering figure underscores the importance of strong passwords, multi-factor authentication, and other measures to protect against credential theft.

Key Statistics - Unit 42

- **Extortion Tactics:** There's a 49% increase in organizations listed on dark web leak sites, indicating a rise in extortion. Harassment tactics are also increasing in cases where extortion payments are made. Data theft was involved in 82% of cases where payments were made in 2023.
- **Impact of Incidents:** Legal and regulatory losses, along with response and recovery costs, were the most prevalent costs for Unit 42's clients. This emphasizes the broad financial and operational impact of security incidents.

Contributing Factors:

- **Unnecessary Exposure:** 75% of ransomware attacks and breaches were rooted in exposed internet-facing assets, highlighting the importance of attack surface management.
- **Insufficient Patch Management:** Unpatched vulnerabilities were a contributing factor in 30.7% of incidents, while unnecessary exposure of internet-facing resources contributed to 22.8% of incidents. These statistics underscore the need for proactive vulnerability management and timely patching to reduce the attack surface
- **Lack of Endpoint Protection:** Insufficient coverage by endpoint protection technology played a role in 13.6% of incidents. This emphasizes the need for comprehensive endpoint security solutions to detect and prevent malicious activity on devices.

Report Comparison

Cybersecurity Statistics: A Comparative View

The Microsoft Report: A Narrative-Driven Approach

The Microsoft report provides insights into the evolving cyber threat landscape and cybersecurity strategies but does not present statistical data comparable to Mandiant or Unit 42. It offers valuable context on trends like the increasing sophistication of nation-state actors, the blurring lines between nation-state and cybercriminal activity, and the rise of AI as both a tool for attackers and defenders.

Incident Discovery: Internal vs. External

- **Mandiant:** Reports that in 2023, **54%** of organizations received initial compromise notification from an external source. For ransomware-related intrusions, the rate of external notification jumps to **70%**. They attribute the high external notification rate for ransomware to the attacker's business model, where a ransom demand is the first notification for many victims.
- **Unit 42:** In contrast, Unit 42 reports that in 2023, **80%** of incident discoveries were internal. They suggest this positive trend may be influenced by the increasing security maturity of their client base, with organizations more effectively detecting compromises internally.

Reconciling the Differences:

- **Scope and Methodology**: As previously noted, differences in data collection, incident definitions, and the types of incidents included in the analysis could contribute to the variation in findings.
- **Client Profiles**: The types of organizations engaging each firm for incident response could significantly influence the results. Unit 42's focus on larger, more security-mature organizations aligns with their higher rate of internal detection.

Cybersecurity Statistics: A Comparative View

Dwell Time: A Race Against the Clock

- **Mandiant:** Global median dwell time in 2023 decreased to **10 days**. In ransomware cases, the median was **5 days** for external notifications and **6 days** for internal detection.
- **Unit 42:** Observes a general **decreasing trend** in dwell time since 2021, but does not offer specific figures for 2023. They emphasize that defenders are getting faster but highlight the need for even greater speed to counter the swift actions of attackers.

Points of Convergence:

- **Downward Trend:** Both Mandiant and Unit 42 highlight a decreasing trend in dwell time, suggesting improved detection capabilities and faster response times.

Unresolved Questions:

- **Specific 2023 Figures from Unit 42**: A direct comparison with Mandiant's 2023 dwell time statistics would require more detailed data from Unit 42.

Cybersecurity Statistics: A Comparative View

Targeted Industries: Points of Focus

- **Mandiant:** Identifies financial services, business and professional services, high tech, retail and hospitality, and healthcare as the most targeted industries in 2023.
- **Unit 42:** Finds the top six targeted industries to be professional and legal services, high technology, manufacturing, healthcare, finance, and wholesale and retail.

Key Observations:

- **Overlap and Consistencies:** There is significant overlap between the industries identified by both firms, indicating shared vulnerabilities and attacker focus on sectors with valuable data. Financial services, high tech, and healthcare are consistent targets across both reports.
- **Categorization Nuances:** Variations in industry categorization could contribute to ranking discrepancies. For example, Mandiant combines business and professional services while Unit 42 lists them separately.

Cybersecurity Statistics: A Comparative View

Extortion and Data Theft: Increasingly Prevalent Threats

- **Mandiant:** Reports data theft in **37%** of 2023 intrusions, with **11%** involving direct monetization of stolen data. They observe a notable rise in data leak site listings and extortion revenue, underscoring the prevalence of these tactics.
- **Unit 42:** Finds **49%** of targets in 2023 knew or had to assume their data was compromised. Non-targeted data theft was observed in **81%** of cases, highlighting the indiscriminate approach attackers often take. The report emphasizes a significant increase in extortion and harassment tactics, particularly in cases where payment was made.

Shared Concerns:

- **Rising Extortion**: Both reports highlight the increasing use of extortion and data theft, marking a concerning trend in the threat landscape.
- **Data Theft Prevalence:** The sources converge on the prevalence of data theft, with Mandiant focusing on direct monetization and Unit 42 highlighting the frequent lack of targeting specificity.

Statistical Caveats:

- **Data Theft Definitions:** As previously mentioned, variations in how data theft is defined across the reports could impact the comparability of these statistics.