Security for Everyone

2023 CYBER SECURITY STATISTICS:

BREACHES, TOP TRENDS, INVESTMENTS

securityforeveryone.com

TABLE OF CONTENTS

1. INTRODUCTION 3

2. TOP TEN DATA BREACHES IN 2023 4

2.1. DarkBeam 4

2.2. Real Estate Wealth Network 5

2.3. Indian Council of Medical Research (ICMR) 6

2.4. Indonesian Immigration Directorate General 7

2.5. MOVEit 8

2.6. UK Electoral Commission 9

2.7. MGM Resorts 10

2.8. 23andMe 11

2.9. Kid Security 12

2.10. T-Mobile 13

3. KEY TRENDS IN 2023 CYBERSECURITY 14

3.1. Strengthening Resilience through Continuous Enhancement 14

3.2. Enhancing Efficiency and Expanding Coverage 14

3.3. Prioritizing Human Elements and Governance 15

3.4. Leveraging Emerging Technologies 15

3.5. Addressing Evolving Threats 16

3.6. Fostering Collaboration and Information Sharing 16

4. 2023'S CYBERSECURITY INVESTMENTS 17

4.1. Cybersecurity Unicorn Startups 17

4.2. Top 5 Cybersecurity Fundings 18

4.3. Top 5 Cybersecurity Acquisitions 19

5. CONCLUSION 20

6. REFERENCES 21

1. INTRODUCTION

In the digital age, the integrity of data and the security of networks stand as paramount concerns for organizations worldwide.

As we delve into the annals of 2023, this report serves as a beacon, illuminating the landscape of cybersecurity with insights into the most prominent data breaches, key trends, and noteworthy investments that shaped the industry. From the breaches that reverberated through sectors to the innovative measures undertaken to bolster defenses, our exploration delves into the intricate tapestry of cybersecurity, offering a comprehensive overview of the challenges and opportunities that defined the year.

As cyber threats continue to proliferate and evolve, organizations are compelled to adopt proactive strategies to safeguard their assets. Through meticulous analysis and examination, this report endeavors to equip readers with a nuanced understanding of the cybersecurity landscape in 2023. By dissecting emerging trends, investment trends, and strategic imperatives, we aim to empower stakeholders with the knowledge necessary to navigate the complexities of cybersecurity and fortify their digital resilience in an era defined by relentless technological advancement and persistent threats.

2. TOP TEN DATA BREACHES IN 2023

2.1. DarkBeam

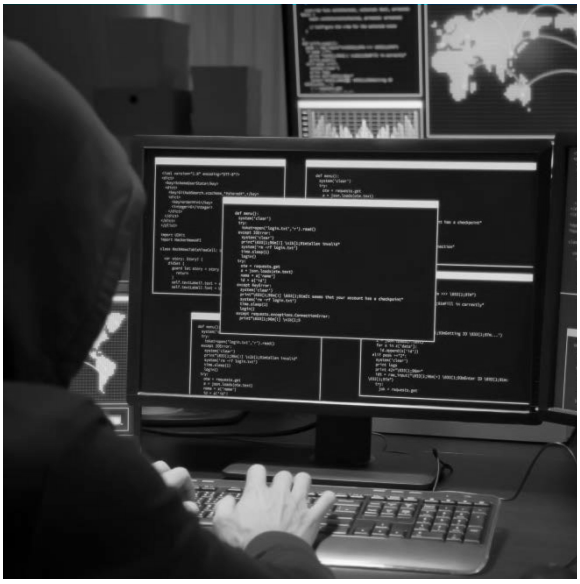
What is DarkBeam?

DarkBeam is a digital risk platform that provides services related to cybersecurity and data protection.

Time: September 2023

Details of the Breach:

The breach involved DarkBeam inadvertently leaving an interface containing the records unprotected. The exposed data included emails and passwords from both previously reported and unreported data breaches, highlighting the extensive scope of the incident.



Data Breached:

More than 3.8 billion records were exposed due to a misconfiguration in the Elasticsearch and Kibana data visualization interface of DarkBeam's platform. This breach compromised various types of sensitive information, including emails and passwords from both previously reported and unreported data breaches.

Response and Mitigation:

Upon being alerted to the breach, DarkBeam swiftly addressed the vulnerability and closed the leak. However, it remains unclear how long the data had been exposed and whether it had been accessed by unauthorized parties with malicious intent.

2.2. Real Estate Wealth Network

What is Real Estate Wealth Network?

Real Estate Wealth Network is a New York-based company that offers educational resources and investment opportunities in real estate, primarily targeting passive real estate investments.

Time: December 2023

Details of the Breach:

The exposed data included comprehensive information on property owners, sellers, investors, and internal user logging data. Among the data were details concerning numerous celebrities, encompassing their street addresses, purchase prices and dates, mortgage company information, mortgage loan amounts, tax ID numbers, and details regarding taxes owed, paid, or due.

Response and Mitigation:

Upon being alerted to the exposure by Fowler, Real Estate Wealth Network swiftly secured the unprotected database to prevent further unauthorized access. This proactive response helped mitigate potential risks associated with the exposure of sensitive property ownership information.

Data Breached:

The exposed database contained over 1.5 billion records, including property ownership data linked to millions of individuals. Upon notification from Fowler, Real Estate Wealth Network promptly took action to secure the exposed database, mitigating the risk of further unauthorized access. This incident underscores the importance of robust data security measures and the vital role played by security researchers in identifying and addressing potential vulnerabilities.

2.3. Indian Council of Medical Research (ICMR)

What is Indian Council of Medical Research (ICMR)?

The Indian Council of Medical Research (ICMR) is a premier biomedical research institution in India that operates under the Department of Health Research, Ministry of Health and Family Welfare.

Time: October 2023

Details of the Breach:

The personal data of approximately 815 million Indian residents, reportedly extracted from the ICMR's Covid-testing database, surfaced for sale on the dark web earlier this month. Security firm Resecurity uncovered the listing, revealing that the compromised data included victims' names, ages, genders, addresses, passport numbers, and Aadhaar numbers (a 12-digit government identification number).

Data Breached:

The breach, totaling 815,000,000 records, emphasizes the dire necessity for robust cybersecurity measures to safeguard sensitive medical and personal data. Such a vast exposure underscores the grave risks to individuals' privacy and accentuates the criticality of proactive steps to thwart unauthorized access and prevent data breaches.

2.4. Indonesian Immigration Directorate General

What is the Indonesian Immigration Directorate General?

The Indonesian Immigration Directorate General is tasked with managing immigration matters in Indonesia, such as passport issuance and regulation.

Time: July 2023

Details of the Breach:

The breach involved unauthorized access to the Indonesian Immigration Directorate General's database, resulting in the leakage of passport data belonging to over 34 million Indonesian citizens. The compromised information included full names, passport numbers, expiry dates, dates of birth, and genders of the passport holders.

Data Breached:

The stolen data, encompassing 34.9 million Indonesian passport holders, was put up for sale for $10,000. A portion of the pilfered data was also shared on a hacker platform, showcasing passport data spanning from 2009 to 2020, with the validity of the data confirmed through a provided sample. The leaked data potentially included National Identity Community Identity Card (NIKIM) information, used for securing electronic passports and containing personal details like names, addresses, and identity numbers.

Response and Mitigation:

While specifics regarding the breach's execution were not disclosed, reports indicated that the breached data was distributed and traded on the bjork.ai website, hinting at a potentially sophisticated cyber attack or hacking operation. Discrepancies in data structure between the breached data and the national data center prompted ongoing investigations to grasp the breach's extent and nature.

2.5. MOVEit

What is MOVEit Transfer?

MOVEit Transfer is a file transfer tool utilized by organizations worldwide to manage the secure transfer of sensitive data over the internet. It is employed across various sectors, including finance, healthcare, and government, to ensure the safe exchange of critical information.

Attackers: cl0p Group

Time: May 2023

Details of the Breach:

The attackers capitalized on the zero-day vulnerability in MOVEit Transfer, gaining unauthorized access to MOVEit servers and exfiltrating vast amounts of sensitive data.

Data Breached:

The breach impacted over 1,000 organizations and more than 60 million individuals globally, with sensitive data compromised across multiple sectors, including education, transportation, and government. The financial implications of the breach were estimated to be substantial, with potential costs escalating to billions of dollars.

2.6. UK Electoral Commission

What is the Electoral Commission?

The Electoral Commission is an independent authority tasked with supervising elections and regulating political finance in the United Kingdom.

The Electoral Commission

Attackers: Hostile Actors

Time: August 2023

Details of the Breach:

Hostile actors executed a complex cyber-attack, gaining unauthorized access to internal emails, control systems, and copies of electoral registers containing voter data.

Response and Mitigation:

In response, the Electoral Commission collaborated with the National Cyber Security Centre (NCSC), law enforcement, and external experts to investigate and fortify its systems. Substantial improvements were made to enhance the security of their IT infrastructure.

Data Breached:

The breach, which began in August 2021, went undetected until October 2022 when suspicious activity was identified. The accessed electoral registers contained the names and addresses of UK voters registered between 2014 and 2022, totaling approximately 40 million individuals per year. Notably, details of anonymous voters were excluded.

2.7. MGM Resorts

What is MGM Resorts?

MGM Resorts International is a prominent global hospitality and entertainment company renowned for its hotels, resorts, and casinos.

Attackers: Scattered Spider and ALPHV Collaboration

Time: September 2023

Details of the Breach:

Researchers uncovered an English-Russian alliance between Scattered Spider and ALPHV, indicating collaboration between hackers from the U.S., U.K., and Russian-speaking Ransomware-as-a-Service (RaaS) groups. This partnership expanded the threat landscape, demonstrating cross-border cooperation in cybercrime. The threat actors accessed the data from a misconfigured and unprotected cloud server left exposed on the internet. Despite the ransom demand, which the company refused to pay, the incident resulted in losses exceeding $100 million.

Data Breached:

The breach compromised the personal and financial details of over 142 million MGM Resorts guests, highlighting the severity of the incident and its far-reaching consequences.

2.8. 23andMe

What is 23andMe?

23andMe offers DNA testing services allowing users to explore their ancestry, discover ethnic backgrounds, and connect with relatives through shared DNA.

Time: October 2023

Details of the Breach:

The breach involved unauthorized access to 23andMe's "DNA Relatives" feature, enabling users to share personal data, including ancestry reports and matching DNA segments, with other users globally. The breach likely occurred through a 'credential stuffing attack,' where bad actors utilized combinations of usernames and passwords from previous data breaches on other websites, exploiting password reuse vulnerabilities.

Response and Mitigation:

23andMe promptly responded by mandating email two-step verification (2SV) for all customers, temporarily disabling certain features within the DNA Relatives tool for enhanced security, and urging users to update their login credentials and enable multi-factor authentication.

Data Breached:

Personal information, including display names, birth years, sex, and details about genetic ancestry results, was exposed. Initially, data of one million users of Ashkenazi Jewish descent and another 100,000 users of Chinese descent were reported stolen. This later extended to include records of four million more general accounts. Notably, genetic data itself was not compromised.

2.9. Kid Security

What is Kid Security?

Kid Security is a popular parental control app designed to assist parents in monitoring and managing their children's online safety.

Time: November, 2023

Details of the Breach:

The breach was first identified by security researcher Bob Diachenko of SecurityDiscovery in mid-September. It affected more than 300 million data records, including 21,000 telephone numbers and 31,000 email addresses. Additionally, some payment card data was exposed.

Response and Mitigation:

More than 300 million records were compromised in the breach, posing a significant risk to the privacy and security of Kid Security users and their families.

Data Breached:

More than 300 million records were compromised in the breach, posing a significant risk to the privacy and security of Kid Security users and their families.

2.10. T-Mobile

What is T-Mobile?

T-Mobile is one of the largest mobile carriers in the United States, providing wireless communications services to millions of customers.

Time: September 2023

Details of the Breach:

1. Employee Data Exposure:

The breach involved the exposure of 89 gigabytes of data primarily related to T-Mobile employees, including email addresses and partial Social Security Numbers. This data was traced back to an earlier breach in April at Connectivity Source, a T-Mobile retailer. T-Mobile clarified that it was not directly hacked, indicating the breach occurred at a third-party service provider. The exposed employee data could potentially lead to identity theft or fraud.

2. Customer Data Exposure:

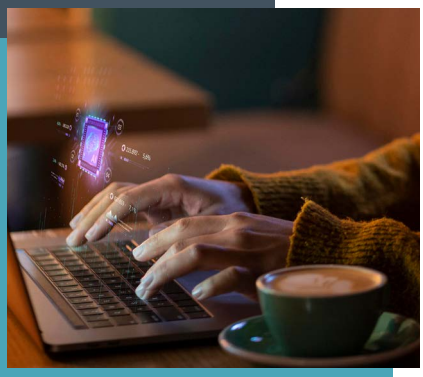
A system error in the T-Mobile app led to the exposure of customer payment data for fewer than 100 customers. Users inadvertently accessed other customers' personal information, including phone numbers and billing addresses, due to a glitch related to a technology update.

Data Breached:

While T-Mobile initially stated that fewer than 100 individuals were affected, subsequent reports suggested that millions of customers' personal information might have been exposed. However, the exact number remains undisclosed by the company.

3. KEY TRENDS IN 2023 CYBERSECURITY

In the dynamic landscape of cybersecurity, 2023 witnessed significant progress in practices that underscore the importance of continuous adaptation, optimization, and a well-balanced approach.



3.1. Strengthening Resilience through Continuous Enhancement

• Threat Exposure Management:

This approach prioritizes ongoing refinement of strategies, involving continuous evaluation and remediation of vulnerabilities.

• Identity Fabric Immunity:

Inspired by the human immune system, it aims to minimize vulnerabilities within identity systems through preventive measures and robust detection and response.

• Cybersecurity Validation:

This practice evaluates the effectiveness of existing security measures against real-world threats and potential attacker behaviors.

3.2. Enhancing Efficiency and Expanding Coverage

• Cybersecurity Platform Consolidation:

This trend focuses on reducing the number of vendors and platforms, streamlining operations, and enhancing integration.

• Security Operating Model Transformation:

This strategic shift distributes security tasks and data analysis across different teams, fostering quicker decision-making.

• Composable Security:

This approach integrates security controls into software architecture, enabling adaptation to changing needs and ensuring protection throughout development.

3.3. Prioritizing Human Elements and Governance

- **Human-Centric Security Design:**

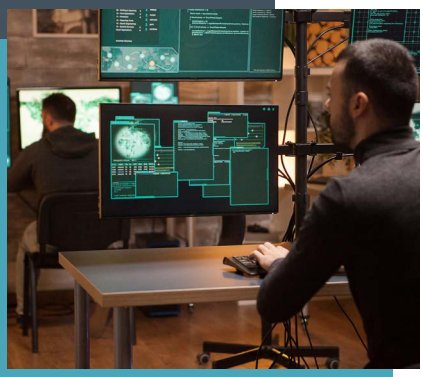
This approach prioritizes user experience in security design, reducing the likelihood of employee behavior becoming a security risk.

- **Enhancing People Management:**

Effective talent management strategies attract and retain skilled cybersecurity professionals, enhancing overall functionality and technical expertise.

- **Increasing Board Oversight:**

This trend encourages active participation of board members in cybersecurity governance, often necessitating additional security expertise within leadership.



3.4. Leveraging Emerging Technologies

- **Harnessing AI and ML:**

Utilizing AI and ML for threat detection, automation of security tasks, and incident response improves efficiency and accuracy.

- **Quantum-resistant cryptography:**

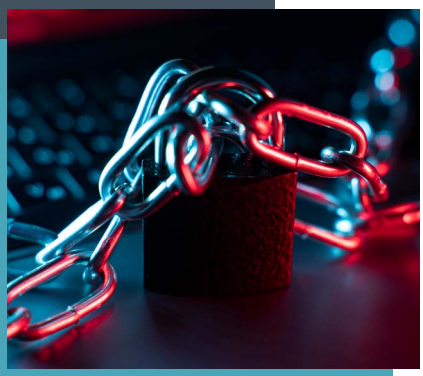
As quantum computing advances, exploring and implementing quantum-resistant cryptographic algorithms becomes crucial for future security.

- **Zero Trust Architecture (ZTA):**

This security model assumes no implicit trust and verifies every user and device attempting to access resources, reducing the attack surface and potential damage.

- **Cloud Security:**

With increasing reliance on cloud services, ensuring robust security measures like encryption and access controls in the cloud environment becomes crucial.



3.5. Addressing Evolving Threats

- **Ransomware-as-a-Service (RaaS):**

As these threats evolve, organizations need comprehensive strategies to identify, prevent, and respond to them.

- **Supply Chain Security:**

Mitigating risks associated with third-party vendors and integrating security measures throughout the supply chain is increasingly important.

3.6. Fostering Collaboration and Information Sharing

- **Public-private partnerships:**

Collaboration between governments, businesses, and security researchers is essential to stay ahead of emerging threats and share best practices.

- **Threat intelligence sharing:**

Sharing threat information between organizations allows for quicker identification and mitigation of widespread attacks.

- **Importance of threat intelligence:**

Continuously gathering and analyzing threat intelligence helps organizations stay informed about the latest threats and vulnerabilities, enabling proactive defense strategies.

These trends underscore the evolving nature of cybersecurity, emphasizing the continual need for adaptation, optimization, and a well-rounded approach that places importance not only on technology but also on human factors and organizational governance.

4. 2023'S CYBERSECURITY INVESTMENTS

4.1. Cybersecurity Unicorn Startups

Cybersecurity companies on The Crunchbase Unicorn Board as of mid-2023 include:

- **Wiz:**

  Offers an automated platform focusing on cloud security, aiding businesses in identifying and rectifying security vulnerabilities and misconfigurations within their cloud infrastructure.

- **Tanium:**

  Delivers endpoint security and management solutions tailored for organizations.

- **Lacework:**

  Specializes in automated threat detection, compliance monitoring, and anomaly detection within cloud computing environments.

- **Fireblocks:**

  Provides a platform for digital asset custody and transfer, assisting organizations in safeguarding and managing digital assets, including cryptocurrencies.

- **Netskope:**

  Develops tools for monitoring and protecting against threats to cloud services, applications, and data.

- **Snyke:**

  Offers a platform aiding software developers in identifying and addressing vulnerabilities in open-source code and containers.

- **1Password:**

Supplies a password manager and digital vault for both consumers and businesses, enabling secure storage, generation, and management of passwords and sensitive information.

- **OneTrust:**

Provides a privacy management platform enabling organizations to manage and demonstrate compliance with data privacy regulations, conduct assessments, and implement data governance practices.

- **Coalition:**

Renders risk management, insurance, and incident response services to businesses, helping them protect against cyber threats and recover from cyber incidents.

- **SonarSource:**

Provides code analysis and inspection tools to assist software developers in identifying and resolving vulnerabilities in their codebases.

4.2. Top 5 Cybersecurity Fundings

The following represents the top 5 Cybersecurity Fundings sourced from Crunchbase search for cybersecurity fundings, indicating significant investments in the sector:

TRANSACTION NAME	ORGANIZATION NAME	TYPE	ANNOUNCEMENT DATE	AMOUNT	LEAD INVESTOR
Venture Round - SandboxAQ	SandboxAQ	Venture Round	14-Feb-23	$500,000,000	–
Convertible Note - Netskope	Netskope	Convertible Note	5-Jan-23	$401,000,000	Morgan Stanley
Series D - Wiz	Wiz	Series D	27-Feb-23	$300,000,000	Greenoaks, Index Ventures, Lightspeed Venture Partners
Series C - Blackpoint Cyber	Blackpoint Cyber	Series C	8-Jun-23	$190,000,000	Bain Capital Tech Opportunities
Series C - Deepwatch	Deepwatch	Series C	15-Feb-23	$180,000,000	–

4.3. Top 5 Cybersecurity Acquisitions

The following represents the top 5 Cybersecurity Acquisitions sourced from Crunchbase search for cybersecurity acquisitions, indicating significant investments in the sector:

TRANSACTION NAME	ACQUIREE NAME	ACQUIRER NAME	ACQUISITION DATE	PRICE
Imperva acquired by Thales Group	Imperva	Thales Group	25-Jul-23	$3,600,000,000
Forcepoint acquired by TPG	Forcepoint	TPG	10-Jul-23	$2,450,000,000
Magnet Forensics acquired by Thoma Bravo	Magnet Forensics	Thoma Bravo	20-Jan-23	$1,800,000,000
ADT acquired by GTCR	ADT	GTCR	8-Aug-23	$1,600,000,000
Absolute Software acquired by Crosspoint Capital Partners	Absolute Software	Crosspoint Capital Partners	11-May-23	$870,000,000

The cybersecurity sector experienced a significant downturn in venture funding in 2023, reaching its lowest levels in five years. Despite this overall decline, a few cybersecurity startups managed to secure substantial funding rounds, including SandboxAQ, Netskope, and Wiz. Industry experts attribute this decline to the aftermath of the exceptional surge in 2021, characterized by inflated valuations and excessive funding rounds. Startups are now grappling with the consequences of past decisions and facing pressure to secure follow-on funding or explore acquisition options. This trend underscores the importance of prudent financial management and strategic planning in the cybersecurity startup landscape.

5. CONCLUSION

The recent surge in data breaches underscores the ever-evolving and relentless nature of cyber threats, highlighting the critical importance for businesses and organizations across all sectors to prioritize and continually enhance their cybersecurity measures. These incidents serve as stark reminders of the potential consequences of inadequate data protection, including damage to reputation and financial losses.

To preemptively safeguard against the looming threat of data leaks or breaches, it is imperative to adopt a proactive approach and implement a robust cybersecurity strategy. By staying two steps ahead of potential attackers, organizations can fortify their defenses and mitigate the risks associated with cyber intrusions.

Key trends have emerged, emphasizing the importance of efficiency, governance, and human elements in bolstering defenses. Simultaneously, the adoption of emerging technologies and the promotion of collaboration were identified as crucial strategies for staying ahead of evolving threats. Investments in innovative cybersecurity solutions demonstrate a proactive stance toward addressing future challenges, highlighting the industry's commitment to proactive risk management and defense.

In conclusion, the recent spate of data breaches underscores the critical importance of prioritizing cybersecurity in today's digital landscape. By embracing proactive security measures and leveraging advanced security solutions like Security for Everyone, organizations can enhance their resilience to cyber threats and safeguard their valuable data and stakeholders' trust.

6. REFERENCES

- Verizon. (2023). "2023 Data Breach Investigations Report" Retrieved from https://www.verizon.com/business/en-nl/resources/reports/dbir/
- ItGovernance. (2023). "List of Data Breaches and Cyber Attacks in 2023" Retrieved from https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
- CyberSecurityNews. (2023). "10 Most Notable Cyber Attacks of 2023" Retrieved from https://cybersecuritynews.com/notable-cyber-attacks-of-2023/
- NordLayer. (2023). "Breakdown of the 12 most significant 2023 data breaches" Retrieved from https://nordlayer.com/blog/data-breaches-in-2023/#key-facts-of-2023s-data-breaches-we-know-so-far
- MsspAlert. (2023). "Top 10 Cyberattacks of 2023" Retrieved from https://www.msspalert.com/news/top-10-cyberattacks-of-2023/
- WeLiveSecurity. (2023). "A year in review: 10 of the biggest security incidents of 2023" Retrieved from https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023/
- Gartner. (2023). "Top Strategic Cybersecurity Trends for 2023" Retrieved from https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Forbes. (2023). "Top Cybersecurity Trends In 2023" Retrieved from https://www.forbes.com/sites/forbestechcouncil/2023/10/17/top-cybersecurity-trends-in-2023/?sh=278f08507e1d
- SimpliLearn. (2023). "20 Emerging Cybersecurity Trends to Watch Out in 2024" Retrieved from https://www.simplilearn.com/top-cybersecurity-trends-article
- Crunchbase. (2023). "Cybersecurity Funding" Retrieved from https://www.crunchbase.com/lists/cybersecurity-funding/65e7f4ce-fbcb-4752-adcb-8d82edfc4639/funding_rounds
- Crunchbase. (2023). "Acquisitions" Retrieved from https://www.crunchbase.com/search/acquisitions/026cb4a07fce8c16502d135f72118cf4
- Crunchbase. (2023). "Cybersecurity News" Retrieved from https://news.crunchbase.com/sections/cybersecurity/