Only AI-Equipped Teams Can Save Data Leaks From Becoming the Norm for Global Powers

15D AGO MORGAN WRIGHT (1 VOTE)

COMMENT FONT SIZE 5.7 MIN READ

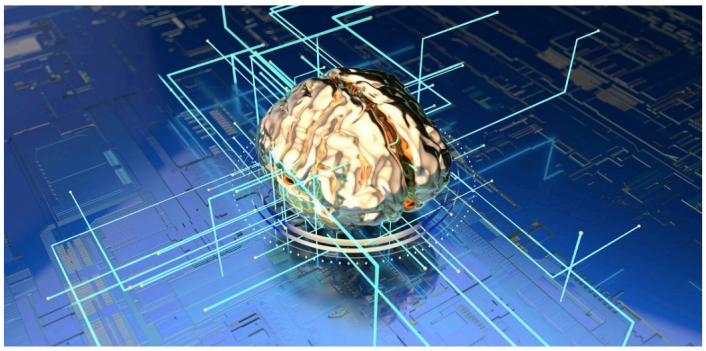

Image Credit: julos/BigStockPhoto.com

In a shocking revelation, a massive data leak has exposed sensitive personal information of over 1.6 million individuals, including Indian military personnel, police officers, teachers, and railway workers. This breach, discovered by cybersecurity researcher Jeremiah Fowler, included biometric data, birth certificates, and employment records and was linked to the Hyderabad-based companies ThoughtGreen Technologies and Timing Technologies.

While this occurrence is painful, it is far from shocking.

The database, containing 496.4 GB of unprotected data, was reportedly found to be available on a dark web-related Telegram group. The exposed information included facial scans, fingerprints, identifying marks such as tattoos or scars, and personal identification documents, underscoring a growing concern about the security protocols of private contractors who manage sensitive government data.

The impact of such breaches goes far beyond what was capable years ago. In the past, stolen identity would have led to the opening of fake credit cards or other relatively containable incidents. Today, a stolen identity that includes biometric data or an image with personal information is enough for threat actors to create a deep fake and sow confusion amongst personal and

professional colleagues. This allows unauthorised personnel to gain access to classified information from private businesses and government agencies, posing a significant risk to national security.

Deepfakes even spread fear throughout southeast Asia, specifically during India's recent Lok Sabha, during which 75% of potential voters reported being exposed to the deceitful tool.

The Risks of Outsourcing Cybersecurity

Governments increasingly rely on private contractors to manage and store vast amounts of sensitive data. However, this reliance comes with significant risks. Private firms often lack the robust cybersecurity measures that government systems can implement.

However, with India continuing to grow as a digital and cybersecurity powerhouse, the hope was that outsourcing the work would save taxpayers money while providing the most advanced technology possible.

However, a breach risks infecting popular software or other malicious actions such as those seen in other supply chain attacks, which are a stark reminder of the need for stringent security measures and regular audits of third-party vendors.

Leveraging AI for Cybersecurity

Cybercrime is on the rise globally, with threat actors becoming more sophisticated in their methods. The growth of AI has further complicated the cybersecurity landscape. While AI offers powerful tools for defence, it also provides new capabilities for cybercriminals who can use it to pry and prod at a system faster than ever before until a vulnerability is found. What's more, this technology can be used to automate attacks, create more convincing phishing schemes, and even develop malware that can adapt and evolve to avoid detection.

While this may sound like the ultimate nightmare scenario, this same technology offers significant advantages to cybersecurity teams. AI-driven tools can automate threat detection and response, reducing the burden on human analysts and allowing them to focus on more complex tasks. For instance, large

THE FAST MODE ANALYTICS

I am here for:

- [ ] Solution Ideas
- [ ] Service Innovation Ideas
- [ ] Daily Market Updates
- [ ] Competitor News
- [ ] References
- [ ] Just Checking Things Out

SUBMIT

language models (LLMs) can process and analyse vast amounts of data quickly, identifying threats in real-time and providing actionable insights.

AI can also play a crucial role in upskilling employees within cybersecurity teams. With the implementation of LLMs, even less experienced team members can make impactful decisions based on AI-driven insights. These models allow analysts to use natural language queries to gather information, eliminating the need for specialised training in various querying languages. By running queries like "Can vulnerability '#123' be found anywhere in the network?" teams can quickly identify potential threats and take appropriate action.

Furthermore, AI assists in automating routine tasks, allowing cybersecurity professionals to focus on strategic initiatives. It can offer next-step recommendations based on previous actions, enhancing the decision-making process. For example, when an alert is triggered, AI can provide insights such as "This alert is typically dismissed by 90% of users" or "An event looks suspicious. Click here to investigate further."

This streamlines operations and accelerates the learning curve for junior analysts, allowing them to quickly become proficient in identifying and mitigating threats, thus leveling up the entire team's capabilities.

Balancing the Scales

As it has always been in the battle between cybersecurity teams and threat actors, there is no one-size-fits-all solution that can secure all networks. However, machine-speed attacks need a machine-speed autonomous response that only AI can deliver.

The recent data leak in India highlights the importance of robust cybersecurity measures, especially when dealing with sensitive government data. As cyber threats evolve, so too must our defences. By leveraging the power of AI, cybersecurity teams can remain one step ahead on the frontlines of protecting government data, digital economies, and even the complex infrastructure that keeps society functioning as it does.

artificial intelligence | data security | network security | cyber security | sentinelone

Morgan Wright

Morgan is an internationally recognized expert on cybersecurity strategy, cyberterrorism, national security, and intelligence. He currently serves as a Senior Fellow at The Center for Digital Government, Chief Security Advisor for SentinelOne, and the chief technology analyst for Fox News and Fox Business. Morgan's landmark testimony before Congress on Healthcare.gov changed how the government collected personally identifiable information. Previously Morgan was a Senior Advisor in the US State Department Antiterrorism Assistance Program, the Senior Law Enforcement Advisor for the 2012 Republican National Convention, taught behavioral analysis at the National Security Agency, and spent a year teaching the FBI how to conduct internet investigations. In addition to 18 years in state and local law enforcement as a highly decorated state trooper and detective, Morgan has developed solutions in defense, justice, and intelligence for the largest technology companies in the world including Cisco, SAIC, Unisys, and Alcatel-Lucent/Bell Labs.

PREVIOUS POST

‹ Push to Eliminate 'Digital Poverty' to Drive Demand for Satellite-Powered Broadband Connectivity Post Pandemic

RELATED CONTENT