LOGICALIS
Architects of Change

Platinum
Business
Partner

IBM

Solution Brief

Cybersecurity Risk Update, 2024: The Global "Identity Crisis"

Logging in with valid credentials is a preferred weapon of choice for cybercriminals – a method of attack made easier with the help of generative AI

According to IBM X-Force®, IBM Consulting's offensive and defensive security services arm, "logging in" with valid credentials is increasingly a preferred weapon of choice for cybercriminals. Exploiting valid accounts has several advantages and is becoming a path of least resistance for several reasons:

Billions of compromised credentials are readily available on the Dark Web

Many organizations fail to implement best practices and security fundamentals

Generative AI is empowering more cybercriminals with a larger set of tools

This type of identity theft poses several problems for defenders. Not only is it harder to detect, it elicits a costly response from enterprises. Credential-based attacks earn a nearly 200% more complex response and an average of roughly 11 months' recovery time - a longer response lifecycle than any other infection vector.

IBM's 2024 X-Force Threat Intelligence Index[1] reported several other alarming findings related to this growing global "identity crisis":

71%
year-over-year increase in volume of attacks using valid credentials

84%
of attacks on critical sectors could have been mitigated with "basic security" measures

266%
surge in the use of info stealing ransomware

> "Identity is being used against enterprises time and time again, a problem that will worsen as adversaries invest in AI to optimize the tactic."
>
> - Charles Henderson
> Global Managing Partner, IBM Consulting, and Head of IBM X-Force

Despite the growing risk of cyber incidents and data breaches, many organizations are stalling on their cybersecurity investments. The 2023 IBM Cost of a Data Breach Report[2], for instance, found that while 95% of organizations have experienced more than one breach, only half (51%) planned to increase their security investments in response.

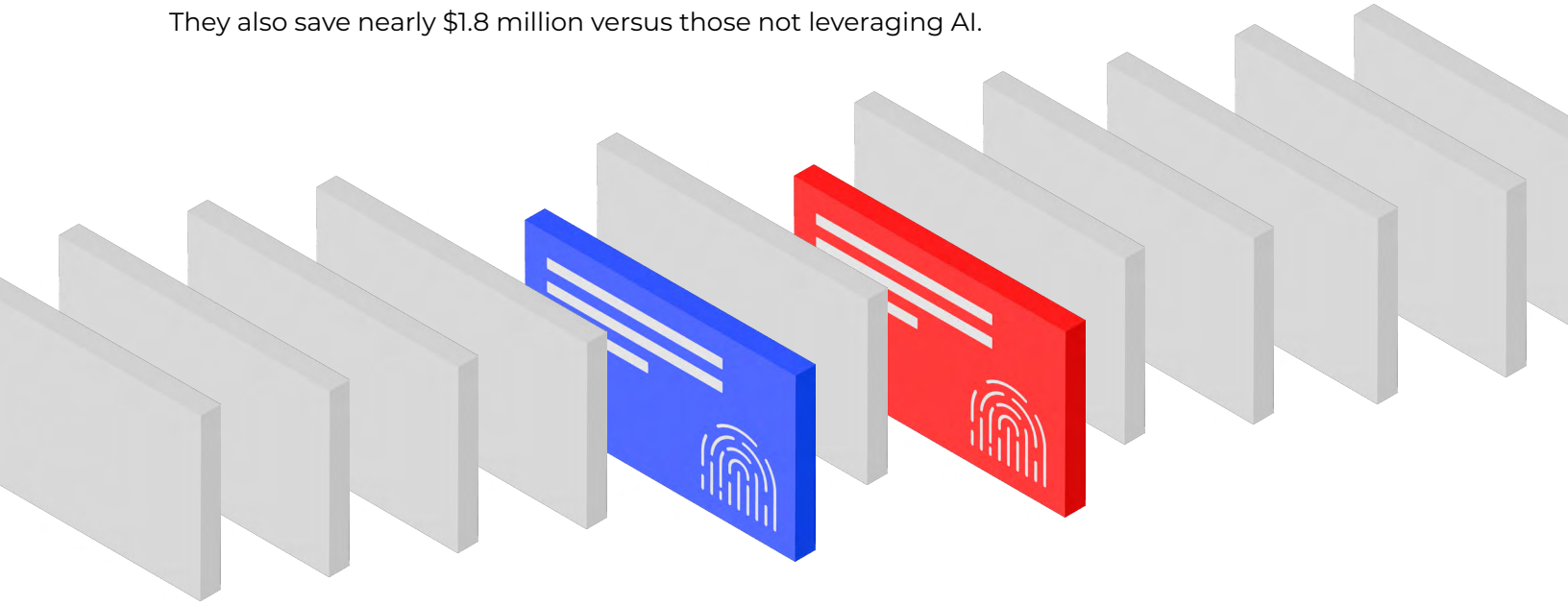
1. https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches
2. https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

Generative AI: The Next Frontier for Cybersecurity

When it comes to cybersecurity, AI is a double-edged sword: it empowers both attackers and defenders.

Hackers, for instance, are using generative AI to create better phishing emails, malware, and more. Generative AI also enables less technically savvy actors to engage in cybercrime, opening the door to a larger pool of cyber attackers to perform malicious tasks, including identity theft. As generative AI becomes more powerful, it is increasingly being used for face swaps, video emulators, and other deepfake-related attacks.

On the other hand, when used properly, generative AI also delivers significant benefits to the blue team. When compared to those not using AI, organizations using AI and automation extensively experience, on average, a 108-day shorter time to identify and contain a breach. They also save nearly $1.8 million versus those not leveraging AI.



Tackling the "Identity Crisis" with the Right Security Solutions

A number of security solutions can help address the burgeoning identity crisis. Here are a few:

Identity and access management (IAM) solutions, such as IBM Security® Verify[3], are becoming increasingly critical in the modern enterprise, and they are becoming critical to addressing identity-based attacks.

Products that offer features such as **User Behavior Analytics (UBA)**, offered through products such as IBM Security® QRadar® SIEM[4], can also help detect and investigate compromised credentials, lateral movement, and other abnormal behavior.

3. https://www.ibm.com/verify

4. https://www.ibm.com/products/qradar-siem/user-behavior-analytics

Endpoint detection and response (EDR), such as IBM Security® QRadar® EDR[5], can also be used to detect anomalous behavior, such as the exfiltration of data or the creation of new accounts or folders on sensitive systems.

The most modern solutions, including most of the offerings from IBM, also use AI to handle a significant portion of the workload, which can free up staff time, lower error rates, decrease costs, and reduce the need for specialized talent.

Addressing the Global "Identity Crisis" in 2024 and beyond

Understanding the threat landscape is crucial to protecting people, data, and infrastructure, but it's only the first step. Action is needed to improve the security posture, be more resilient, and stay ready for cyber threats, today and tomorrow.

Logicalis, a Platinum IBM Partner with extensive expertise in cybersecurity, is a global Managed Service Provider that has helped organizations integrate, implement, manage, and maintain enterprise-grade security systems with IBM.

To learn more about IBM's security solutions, contact us today to schedule a free executive briefing.

5. https://www.ibm.com/products/qradar-edr