When it comes to cybersecurity, fight fire with fire

Generative AI is unlike any technology that has come before. It's swiftly disrupting business and society, forcing leaders to rethink their assumptions, plans, and strategies in real time.

To help CEOs stay on top of the fast-shifting changes, the IBM Institute for Business Value (IBM IBV) is releasing a series of targeted, research-backed guides to generative AI, on topics from data cybersecurity to tech investment strategy to customer experience.

This is part seven: Cybersecurity.

Generative AI amplifies risk—and resilience

Generative AI has given rise to a new generation of cyber threats. Hackers have more opportunities to exploit vulnerabilities—and more ways to execute their malicious campaigns.

Fortunately, the opposite is also true: Generative AI can fortify business defense. In the near term, generative AI will speed up security processes that were once a heavy lift. And by analyzing vast amounts of data and recognizing patterns—and anomalies—generative AI can spot threats as quickly as they materialize.

As bad actors add new tricks to their repertoire, cybersecurity teams will need to move fast to keep pace. In this game of cat-and-mouse, vigilance will be the key to managing vulnerabilities—and staying a step ahead.

The IBM Institute for Business Value has identified three things every leader needs to know:

1. Generative AI ushers in a world of new risks and threats.
2. Trustworthy generative AI is not possible without secure data.
3. Using generative AI for cybersecurity is a force multiplier.

And three things every leader needs to do right now:

1. Treat generative AI like a burning platform and secure it now.
2. Make trusted data the backbone of your organization.
3. Reorient cybersecurity investments around speed and scale.

1. Cyber-risk + Generative AI

What you need to know

Generative AI ushers in a world of new risks and threats

Generative AI has given cyber attackers a whole new arsenal. Hackers are no longer just spoofing emails—today they can mimic voices, faces, and even personalities to trick victims into falling into their traps.

And this is just the beginning.

As generative AI proliferates over the next six to 12 months, experts expect new intrusion attacks to exploit scale, speed, sophistication, and precision, with constant new threats on the horizon. When considering both likelihood and potential impact, autonomous attacks launched in mass volume stand out as the greatest risk. However, executives expect hackers faking or impersonating trusted users to have the greatest impact on the business, followed closely by the creation of malicious code.

How organizations implement generative AI could introduce new risks, as well. In fact, 47% of executives are concerned that adopting generative AI in operations will lead to new kinds of attacks targeting their own AI models, data, or services. And almost all executives (96%) say adopting generative AI makes a security breach likely in their organization within the next three years.

With the average cost of a data breach reaching $4.45 million globally—$9.48 million in the US—companies are investing heavily in managing new cybersecurity risks. Executives say their 2023 AI cybersecurity budgets are 51% greater than they were in 2021. And they expect those budgets to climb an additional 43% by 2025.

Executives say their 2023 AI cybersecurity budgets are **51% greater** than they were in 2021.

And they expect those budgets to climb an **additional 43%** by 2025.

1. Cyber-risk + Generative AI

What you need to do

Treat generative AI like a burning platform and secure it now

Pressure cybersecurity leaders to act with urgency, responding to generative AI's risks as immediate—not incremental.

Understand your AI exposure. Convene cybersecurity, technology, data, and operations leaders for a board-level discussion on evolving risks, including how generative AI can be exploited to expose sensitive data and allow unauthorized access to systems. Get everyone up to speed on emerging "adversarial" AI—nearly imperceptible changes introduced to a core data set that cause malicious outcomes.

Secure the entire AI pipeline. Focus on securing and encrypting the data used to train and tune AI models. Continuously scan for vulnerabilities, malware, and corruption during model development, and monitor for AI-specific attacks (e.g., data poisoning and model theft) after the model has been deployed.

Invest in new defenses specifically designed to secure AI. While existing security controls and expertise can be extended to secure the infrastructure and data that support AI systems, detecting and stopping adversarial attacks on AI models requires new methods.

2. Data + Generative AI

What you need to know

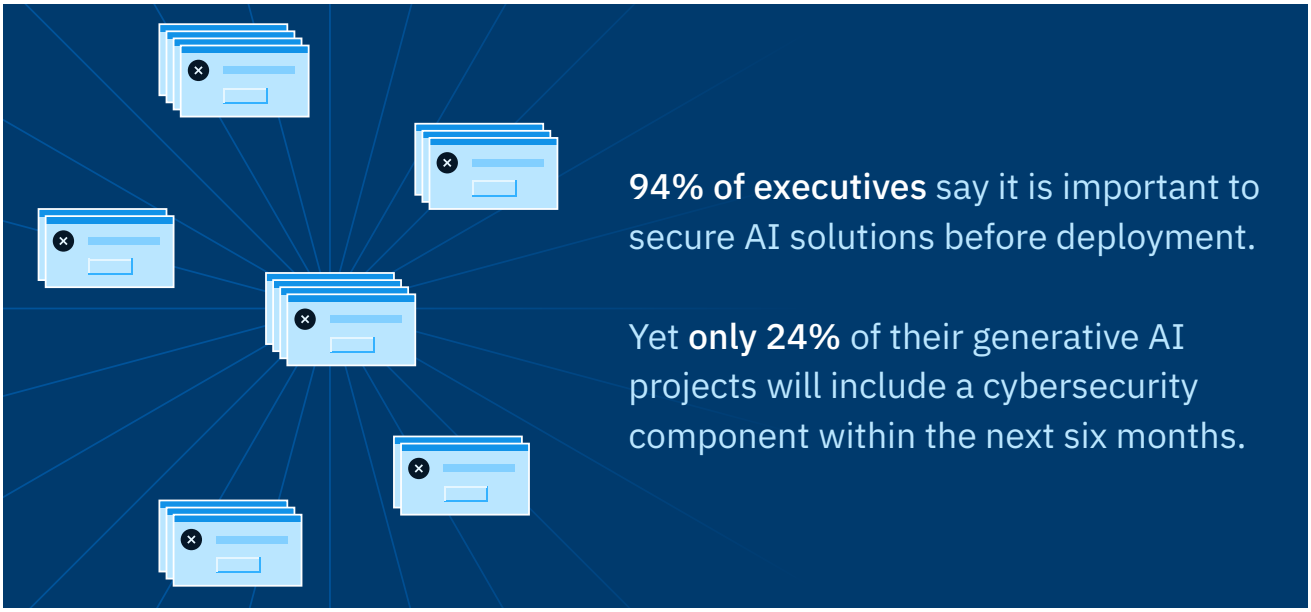
Trustworthy generative AI isn't possible without secure data

Data is the lifeblood of generative AI. All models rely on data to answer queries and inform insights—which is why training data has become a target for cyber attacks. While hackers still want to steal data to sell to the highest bidder, data infiltration offers a new path to ill-gotten gains. If they can change the data driving an organization's generative AI model, they can influence business decisions with targeted manipulation or misinformation. This evolving threat introduces a whole host of new legal, security, and privacy concerns that CEOs will need to manage enterprise-wide.

Executives see the writing on the wall. As they adopt generative AI, they expect a wide variety of risks to materialize, with 84% concerned about widespread or catastrophic cybersecurity attacks that could introduce new vulnerabilities. One in three executives say these risks can't be managed without fundamentally new forms of governance, such as comprehensive regulatory frameworks and independent third-party audits.

Overall, 94% of executives say it is important to secure AI solutions before deployment. Yet only 24% of their generative AI projects will include a cybersecurity component within the next six months—and 69% say innovation takes precedence over cybersecurity for generative AI.

This shows a glaring disconnect between the understanding of generative AI cybersecurity needs and the implementation of cybersecurity measures. To prevent expensive—and unnecessary—consequences, CEOs need to address data cybersecurity and data provenance issues head-on by investing in data protection measures, such as encryption and anonymization, as well as data tracking and provenance systems that can better protect the integrity of data used in generative AI models.



2. Data + Generative AI

What you need to do

Make trusted data the backbone of your organization

Evolve your cybersecurity practices to consider the requirements of multiple generative AI models and data services.

Build trust and security into AI use. Prioritize data policies and controls centered on security, privacy, governance, and compliance. Communicate how transparency and accountability are critical to prevent bias, hallucinations, and other concerns while managing risk.

Protect the data that powers AI. Task your CISO to discover and classify sensitive data used in training or fine tuning and implement data loss prevention techniques to prevent data leakage through prompts. Enforce access policies and controls around machine learning data sets. Expand threat modeling to cover generative AI-specific threats like data poisoning and outputs containing sensitive data or inappropriate content.

Treat cybersecurity like a product. And stakeholders like customers. Cybersecurity has a critical role to play in securing the AI initiatives that will drive revenue. To secure the AI that you use in products, educate your teams on the cybersecurity threats that come with generative AI. Highlight the value of changing behaviors to improve data and security hygiene. Encourage adoption by aligning cybersecurity outcomes to business outcomes.

3. Cyber-resilience + Generative AI

What you need to know

Using generative AI for cybersecurity is a force multiplier

When applied to cybersecurity, generative AI can be a business accelerator. It can automate repetitive and time-consuming tasks, freeing up teams to focus on the more complex and strategic aspects of security. It can also detect and investigate threats and learn from past incidents to adapt the organization's response strategies in real time.

With so much to gain, CEOs are under pressure to introduce generative AI quickly and broadly. But to avoid the collapse of a growth-fueled house of cards, it's imperative that business leaders also use the technology to build resilience. In that way, execs not only avoid the risks of generative AI, they also use it to make their organizations stronger.

More than half of executives (52%) say it will help them better allocate resources, capacity, talent, or skills, and 92% say they are more likely to augment or elevate than replace their cybersecurity workforce as they adopt generative AI.

These new tech tools can help teams reduce complexity and focus on what matters most, which may be why 84% of executives plan to prioritize generative AI cybersecurity solutions over conventional cybersecurity solutions.

And using generative AI in cybersecurity can extend the multiplier effect across your enterprise ecosystem. 84% of executives say that open innovation and ecosystems are important for their future growth strategy. As these leaders look to build relationships that support innovation and growth, most expect generative AI capabilities will influence their selection of ecosystem partners in cloud (59%) and across the business (62%) over the next two years.

As generative AI continues to mature, its potential to deliver value while mitigating risks will only grow. Companies that have built broad capabilities in both risk and resilience will be able to go farther faster with this new technology—and be better positioned to defend future growth.

84% of executives plan to prioritize generative AI cybersecurity solutions over conventional cybersecurity solutions.

3. Cyber-resilience + Generative AI

What you need to do

Reorient cybersecurity investments around speed and scale

Make AI an essential tool to strengthen security defenses. Encourage cybersecurity leaders to embed generative AI and automation into their toolkits to resolve security risks and incidents at speed and at scale. This will provide significant productivity gains and leverage cybersecurity as an enabler for business growth.

Use AI to speed up security outcomes. Automate routine tasks that don't require human expertise and judgment. Use generative AI to streamline tasks that rely on the collaboration between humans and technology, such as security policy generation, threat hunting, and incident response.

Deploy AI to detect new threats. Update tools and techniques to equip your teams with the same speed, scale, precision, and sophistication as your attackers. Use generative AI to identify patterns and anomalies faster, allowing teams to recognize new threat vectors before they disrupt the business.

Find strength in numbers. Work with trusted partners to help define your AI security maturity and implement a comprehensive generative AI strategy that drives value across your organization.

IBM Institute for Business Value

The CEO's guide to generative AI

Cybersecurity

The statistics informing these insights are sourced from four proprietary surveys conducted by the IBM Institute for Business Value in collaboration with Oxford Economics, as well as one reference from the 2023 IBM *Cost of a data breach* report, and one from *Open the door to open innovation* (2022). The first survey was fielded with 200 US-based executives in September–October 2023 regarding generative AI's impact on cybersecurity. The second survey included 414 US-based executives in May–June 2023 on the topic of generative AI's impact on hybrid cloud. The third survey was fielded with 200 US-based executives in August–September 2023 regarding generative AI and AI ethics. The fourth survey asked 300 US-based executives in May 2023 about the impact of generative AI on labor.

ibm.co/ceo-generative-ai-cybersecurity

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | October 2023

DBMQB8RE-USEN-00