Protecting Your Company

from the Rise in AI Cyber Attacks

Avilar Technologies, Inc. | 6760 Alexander Bell Drive, Suite 105 | Columbia, MD 21046 | (888) 759-7053 | www.avilar.com

This year marks a significant milestone in cybersecurity awareness, highlighting the importance of safeguarding digital assets and data from cybercrime. As cybercriminals continuously evolve their tactics, techniques, and procedures (TTPs) to exploit vulnerabilities in systems and networks, one emerging factor is reshaping the cybersecurity landscape: generative artificial intelligence (AI).

Since the rise of generative AI tools like ChatGPT, the cybersecurity field has entered a new era, influencing both attackers' methods and defenders' strategies. Here are seven key steps to help protect your organization from the growing threat of AI-powered cyberattacks.

How Generative AI is Changing Cyberattacks

Generative AI is a branch of AI that creates new content, in response to a human or programmed prompt, based on analyzing a massive amount of existing content. Generative AI can create new text, videos, images, and other content. Cybercriminals are using that capability to generate content and communications to maliciously target victims in defined geographies, demographics, and even organizations.

Because the AI-generated content is so like that created by humans, it's very difficult for readers/users to discern the creator. This becomes particularly problematic when generative AI is used to create convincing scams. One article from Comcast Business explains, "Generative AI can create fraudulent content and digital interactions, including real-time conversations, to impersonate users and elevate social engineering and phishing attacks. It also enables non-native English speakers to refine messages and avoid common linguistic pitfalls." The article urges people to be alert to these 4 fakes:

ONE: Fake Digital Content

Fake digital content including avatars, social media profiles, and malicious websites that can be used to collect credentials and user information.

TWO: Video Deep Fakes

Video deep fakes that can trick users into divulging credentials, potentially undermining the effectiveness of employee cybersecurity training.

THREE: Voice Deep Fakes

Voice deep fakes that simulate the voices of managers and senior executives, leaving fraudulent voice memos or other communications with instructions for staff.

FOUR: Fake Documents

Fake documents that look like authentic documentation and authorizations, designed to breach defenses.

7 Ways to Boost Your AI Cybersecurity

It's always been true that, for cyber resilience, each of us has a part to play.

Partners for the National Cyber Security Month, the Cybersecurity and Infrastructure Security Agency (CISA) and National Cybersecurity Alliance, urge businesses to take these four steps to be cyber resilient:

ONE: Teach Employees to Avoid Phishing

According to the 2023 Comcast Business Cybersecurity Threat Report, phishing is the leading cyber-attack, with nine out of 10 attempts to breach networks starting with a phish. Phishing is when a perpetrator sends an email or text designed to lure unsuspecting recipients into clicking on a link and submitting information so the attacker can gain access to a system with private data. A phishing attack can cause extensive financial harm to individuals and companies.

HOW TO TAKE ACTION: Start by reviewing your existing training on cybersecurity and phishing. Add or update content to reflect today's threats and tactics. Consider making the training mandatory for all employees, at all levels, at least annually. Complement the training with communications you regularly share with the team, so they know what to do and who to contact if they receive a suspicious message. Doing so will help turn your greatest cyber vulnerability (your workforce and contractors) into a cyber strength.

TWO: Require Strong Passwords

Stolen or weak passwords are still one of the main ways that malicious cyber actors gain access to applications and networks. Strong passwords can help to safeguard the data and prevent access. Long, random, unique passwords are the strongest.

HOW TO TAKE ACTION: If you're using passwords at your organization, require strong passwords and regular password updates. A reputable password manager can help individuals keep track of their unique passwords. Also, look into the use of passkeys, alternatives passwords that provide faster, easier, and more secure sign-ins to websites and apps. As the FIDO Alliance explains, "Unlike passwords, passkeys are always strong and phishing-resistant."

THREE: Require Multi-Factor Authentication

Multi-factor authentication (MFA), also known as "two-factor authentication" or "two-step authentication," adds a layer of security by requiring a second verification when logging into an account. The second verification may be a one-time code texted to a phone, emailed to a predefined address, or generated by an authentication app. Biometrics (facial recognition or a fingerprint) or a security key may also be used as the second verification — especially in secure facilities that prohibit the use of personal phones.

HOW TO TAKE ACTION: Require MFA for on-site and remote employees, contractors, and anyone else that may access your organization's systems. This is another "hassle" that most people accept as necessary to protect personal and company data.

FOUR: Keep Business Software Updated and Patched

Cyber criminals are experts at exploiting software vulnerabilities to access systems and acquire data. Software developers routinely create updates and patches to address security vulnerabilities — and it's imperative that organizations apply them. ServiceNow reports that 60 percent of organizations have been victims of a cyber breach due to unpatched vulnerabilities where patches were available.

HOW TO TAKE ACTION: Create an inventory of authorized hardware and software for your organization and remove any unauthorized hardware or software. For operating systems and applications, monitor, test, and deploy the latest updates; enable as many automatic updates as practical. Educate and remind employees to set up automated updates on their own devices. Have them work with your IT team for approval and support before adding new software or apps on company devices.

In addition to these 4 suggestions, here are three additional ways to combat AI cyberattacks and other cyber threats at your organization.

FIVE: Upskill Your Cyber Professionals

It helps to have designated personnel who are responsible for managing the cybersecurity policies, tools, and procedures at your organization. Threats, vulnerabilities, TTPs, and cyber defense best practices are rapidly changing and it's essential that your cyber team stays ahead of the cyber criminals.

HOW TO TAKE ACTION: Ensure that your cyber professionals are learning about the latest tools and practices. Give them ample opportunity to build their skills, so they are practiced at monitoring, identifying, and responding to threats and attacks. If they aren't yet expert in AI, pursue upskilling opportunities so they are fully armed against AI cyberattacks.

SIX: Update Your Business Continuity Plan

The best business continuity plans recognize cyber attacks as one threat the business needs to prepare for. Ideally, there are consistent approaches to monitoring threats, protecting the business, and communicating with others across a wide

range of threats — with the details changing for each threat category.

HOW TO TAKE ACTION: Be sure your business continuity and cybersecurity personnel are acquainted and working together. Review your Business Continuity Plan and protocols with the team. Update to reflect your current threat landscape, vulnerabilities, and response best practices.

SEVEN: Harness AI for Cyber Defense

According to a 2023 IBM report, organizations with extensive use of both AI and automation experienced a data breach lifecycle that was 108 days shorter compared to studied organizations that have not deployed these technologies (214 days versus 322 days). As quickly as cyber criminals are exploiting AI, software companies are building cyber defense systems that harness AI to better thwart their attacks.

HOW TO TAKE ACTION: Have your IT and cybersecurity leaders assess the cyber defense tools you have in place. Identify gaps in the way your organization is monitoring for, identifying, mitigating, and responding to cyber threats. Explore and adopt AI-powered cyber defense tools that will strengthen your organization's cyber resilience.

Awareness, vigilance, and proactive moves can go a long way toward protecting your organization and workforce. The good news is that many of the most effective tools to prevent a breach are relatively easy to implement. It's more a matter of education and action to put those tools into everyday practice.

If you're looking to reduce the risk of AI cyberattacks and building cybersecurity knowledge, skills, and behaviors at your organization, see how a competency-based approach can help. Contact us to start the conversation!

About Avilar

Avilar – The Competency Company™ is a leader in workforce development and planning with web-based competency management and learning solutions for corporations, government, and non-profit organizations. In 1997, Avilar pioneered its award-winning WebMentor™ product line and has built itself on the basis of superior customer service and highly adaptable product design.