paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

When It Comes to Cyber Resilience and AI, Be Sure to Stretch the Limits of Your Imagination

By Haider Pasha, Chief Security Officer, EMEA and LATAM, Palo Alto Networks

In the aftermath of the tragic fire that killed three Apollo 1 astronauts in 1967, a US congressional hearing was convened to discuss the cause and what to do about it. Frank Borman, a highly respected astronaut, testified before the committee and was asked a straightforward question: "What caused the fire?"

Instead of giving an answer laced with technical details, he responded simply and eloquently: "A failure of imagination."

What I'd like to tell all my cybersecurity colleagues and their bosses is that we are in greater jeopardy than ever at compromising our cyber resilience—our ability to rebound immediately and fully from a cyberattack with minimal operational impact—unless we stretch our imaginations. And the inspiration for that effort is both a threat *to* us and a force multiplier *for* us: artificial intelligence (AI).

On the one hand, AI has been leveraged extensively and expertly by cybercriminals, from rogue nation-states and malicious insiders to lone wolf hackers. Other than perhaps their own persistence, it is probably their strongest weapon. On the other hand, however, it is our greatest asset and our best hope to stay one step ahead of the attackers … if we use our imagination.

Threats to Our Resilience

Two years ago, I wrote about cybersecurity in a post-COVID world. Although the pandemic was not officially "done" when I wrote those pieces, I stressed the need for CISOs and CIOs to put in place plans to ensure stronger cybersecurity and cyber resilience when we had finally blunted COVID. Why? It was clear that another viral threat could emerge in the future, and we had to make sure we could withstand its impact. After all, cyberattackers had learned things too.

Then came generative AI.

Think back a few short years, when rootkits could be easily obtained on the dark web, often triggered by phishing emails that were crude and amateurish. Now, hackers use broadly available and much more sophisticated GenAI tools like ChatGPT. Remember those phishing emails replete with spelling, grammar, punctuation, and syntax errors? Gone. All the hackers needed to do was ask ChatGPT to craft them a spotless email.

Another important threat to our resilience is one we've seen and experienced in the past, except now it's on hyperdrive. I'm talking about presidential elections—but not just here in the US. During 2024, there will be more than 60 elections around the world where a state leader will be selected. What a field day for political hackers who want to sow discord among populations with disinformation, deepfakes, and cherry-picked messaging tailored to the biases and fears of a single voter.

I probably don't even need to bring up AI-inspired ransomware against our financial institutions. Even with the state-of-the-art cybersecurity defenses banks and other repositories of wealth and sensitive data have erected, the bad guys keep coming, thanks to their sophisticated and creative use of AI and ML algorithms.

What We Need to Do

For those of us—CISOs, business executives, and cybersecurity industry leaders—charged with ensuring our systems are up and running and our data is protected, it's essential to define what "good" looks like when it comes to cyber resilience.

One thing is clear: We must be able to block even the most sophisticated attacks without involving a single human being, if necessary. I'm not saying we don't need great cyber sleuths and deeply committed security analysts; we certainly do. But we have to abandon the mindset that says we can't trust AI without direct human intervention. We have to trust the AI model. If AI tells us that a firewall indicates a problem, we must accept that and proactively block the potential attack. No time to do manual triage to tell us if it's a credible attack or a false positive. A second's delay can be catastrophic. Humans can and should augment AI models—and, of course, train them—but they can't be a bottleneck. Our goal must be to get as close to near-real time as possible, and we can't do that without AI.

We also must reimagine our approach to managing business risk. It's not just where our organizations are today with an expanding attack surface, dealing with runaway data proliferation, supporting the anywhere/anytime workforce, managing complex supply chains, and meeting spiraling regulatory demands. It's that those are all going to be more complex and critical year after year.

We also should reimagine our security frameworks. It's not just technologies or processes, but entire strategies for cybersecurity and resilience. Modernized, forward-thinking metrics are needed to properly measure security efficacy. If we can't tell ourselves—let alone our C-suite colleagues and our board members—whether our efforts are actually working, we're lost.

Finally, our threat response has to be faster, more automated, more intelligent, and more context-driven than ever. Do we want to chase down every alert as though it represented a direct threat to our survival or handle each alert with the same gravity?

AI Changes How We Do Security

The best way to understand what AI can do for our adversaries and our customers is to actually get your hands around it. We've been engineering AI into our products at Palo Alto Networks for more than a decade. AI provides a tremendous boost for us—both as a leading cybersecurity technology partner and as a large potential point of attack for criminals—in several ways.

It helps us and our customers supercharge security teams to be more effective and efficient—a must-have capability as the pace of change in security threats accelerates. It also helps organizations block sophisticated attacks without human intervention.

In order to do this, organizations must:

- **Capture and manage the right data**. Having a ton of data isn't necessarily the answer; you need relevant, contextually appropriate data in order to make the most of AI for cybersecurity.
- **Adopt a platform approach**. Again, "more technology" isn't what we should be after. Instead, that technology should be engineered and deployed in a way that breeds efficiency, intelligence, and quick reaction—not just a bunch of disparate tools stitched together.
- **Exploit deep expertise**. That expertise must be in the form of human intelligence and, of course, artificial intelligence. The AI component is becoming clearer each day to CISOs, CIOs, and their business-side colleagues. But the human intelligence remains critical, and is unleashed from mundane tasks and drudge work by AI-driven automation tools that help our smart and dedicated staff do things that until recently seemed, well, unimaginable.

Call to Action: An Executive Checklist for Deploying AI for Cyber Resilience

I like to think and act in a way that gives my colleagues and my teams real actionable steps to address problems and exploit opportunities. My very inelegant way of explaining that is, "So what?"

I've just taken a few minutes of your day to give context to a problem I know you all live around the clock and to offer perspectives on why this needs to be addressed. Now, I'll give you my "so what" ideas on what your organization can do in using AI effectively and safely for cyber resilience.

Step 1: Document all your internal AI risks. This may be the one area where stretching your imagination may be the hardest to accomplish, but will pay the biggest dividends in cyber resilience. It's extremely difficult to account for all internal AI risks without a detailed methodology to handle this, and for everyone's buy-in. For instance, I imagine everyone reading this is using LLMs. But are you ensuring that you don't let public LLMs access your source code?

Step 2: Know the ins and outs of AI data. Do you know which browser plugins or tools use AI? Are you aware that Grammarly reads all emails using AI? (These are not rhetorical questions.)

Step 3: Develop an external register of AI risks. For instance, where does the Zoom AI meeting summary go? Does the HR chatbot have access to salary or health information? If you don't know, find out fast.

Step 4: Catalog all the AI services your enterprise should and should not be using. Creating this database is essential, but it doesn't stop there. How do you keep it up to date? After all, this is not a static asset.

Step 5: Develop an organization-wide AI policy. For all you weekend do-it-yourselfers, think of AI like a chainsaw. It's a great tool, but when it's not used properly, it can be incredibly dangerous. Everyone in your organization should understand what they can and can't do with AI, and why.

Step 6: Partner with a trusted cybersecurity leader. Your tools are only as good as the technology partners behind them. As I mentioned earlier, deploying an AI-enabled platform based on the principle of "Simplify, Integrate, Scale" for your AI usage is a smart bet.

Frank Borman's prescient advice to the US space community more than 50 years ago took hold. The National Aeronautics and Space Administration (NASA) completely reimagined their definition and strategy toward risk, as well as the tools, systems, and philosophies they used to fight and defeat risk.

We can all do the same with our strategic and innovative use of AI to create a more cyber-resilient mindset, and to fight off smarter attackers and a higher-stakes set of threat vectors.

Let's just hope it doesn't take a tragedy on the scale of Apollo 1 to force us to use our imaginations.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_article_when-it-comes-to-cyber-resilience_031424