Fynd

The Attack Surface of Change

Attackers now use AI to do most of their work. Every company that transforms with AI opens new doors. Boards must treat security as part of the change, not something added after it.

Farooq Adam, Founder of Fynd

3 November 2026 · 3 min read

What new door does this change open, and who is watching it?

1 The First AI-Run Attack

In September 2025, Anthropic detected something new. A state-sponsored group had turned an AI coding agent into an attack team. The AI ran reconnaissance, wrote exploit code, harvested credentials and pulled out data. It went after about thirty organisations around the world: technology companies, banks, chemical manufacturers and government agencies. A small number of attacks succeeded. By Anthropic's estimate, the AI did 80 to 90 percent of the work. Humans stepped in only at a few decision points.

Anthropic called it the first documented case of a large-scale cyberattack executed without substantial human intervention. It will not be the last.

2 The Attacker's Cost Is Falling Too

In my previous article, I argued that AI is taking the cost of software toward zero. The same is true for attacks. A campaign that once needed a skilled team for months now needs a few operators and an AI agent. Verizon's 2026 Data Breach Investigations Report found that exploited software flaws are now the most common way in, at 31 percent of breaches, for the first time in the report's 19-year history. It also found that AI is shrinking the time defenders have to fix a flaw from months to hours.

India is not a spectator. CERT-In handled more than 29.44 lakh cyber incidents in 2025. IBM's 2026 study puts the average cost of a data breach in India at a record ₹25.5 crore, up 15.9 percent in one year. The same study found that 26 percent of malicious breaches in India were AI-generated.

3 Transformation Widens the Door

Here is the part most boardrooms miss. The attack surface is not only growing because attackers are better. It is growing because of the changes we are making.

Every transformation project adds new doors. An AI agent that can place orders is also an agent that can be tricked into placing the wrong ones. A system that writes its own code can also write a flaw. A new integration between the store, the warehouse and the ERP is also a new path from the internet to the core of the business. Each new supplier connection is another way in: Verizon found that a third party was involved in 48 percent of breaches.

© 2026 Shopsense Retail Technologies Limited. All rights reserved.

There is also the AI nobody approved. Verizon reports that the share of employees who use AI tools often rose from 15 percent to 45 percent in one year. IBM found that unapproved "shadow AI" added ₹1.79 crore on average to the cost of a breach in India where it was present.

So every company has two estates to defend. The **existing estate** is the old ERP, the point-of-sale systems in thousands of stores, the factory controllers and the vendor links that were never designed for this threat. The **future estate** is the AI agents, the generated software, the new data flows and the machine customers. Attackers will look for the seam between the two.

4 Security Is Part of the Change

The old habit was to build first and secure later. That habit was costly before. Now it is dangerous, because attackers move at machine speed and an AI agent can do a great deal of damage in the hours before a human notices.

The good news is that the same technology helps defenders. IBM found that Indian companies that used AI and security automation extensively paid ₹21.3 crore per breach on average, against ₹31.6 crore for those that did not. Defence that runs at machine speed is now possible. It must be designed in from the first day of the project, not bolted on after the launch.

For a CEO, this changes the transformation plan. The question is no longer only "What will this change give us?" It is also "What new door does this change open, and who is watching it?"

In my next article, I will set out what businesses should demand of the partners who lead them through this change.

Farooq Adam is the Founder of Fynd.

Sources

Anthropic, "Disrupting the first reported AI-orchestrated cyber espionage campaign", 13 November 2025.
https://www.anthropic.com/news/disrupting-AI-espionage
Press Information Bureau, Government of India, "CERT-In: India's Frontline Defender against Cyber Threats", 23 January 2026.
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537&lang=1&reg=3
IBM India, "India Records its Highest Average Cost of a Data Breach 2026", 3 August 2026.
https://in.newsroom.ibm.com/India-Records-its-Highest-Average-Cost-of-a-Data-Breach-2026
Verizon, 2026 Data Breach Investigations Report, 19 May 2026.
https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

The series

1. If Software Were Free, Would Anyone Change?
2. The Attack Surface of Change · current
3. Choose Partners Who Can Defend and React

Read the series online at secure.fynd.space/insights

© 2026 Shopsense Retail Technologies Limited. All rights reserved.