

WE'VE ALL HEARD HOW ARTIFICIAL INTELLIGENCE will increase the speed and scale of cyberattacks. Receiving less attention is that attackers can now spend less time developing exploits and more time studying their targets the way sophisticated investors, consultants or competitors do. They can study a company's business model and dependencies, looking for moments of heightened vulnerability. Then they can engineer incidents designed to maximize pressure.

Five emerging cyber incident trends will create particularly challenging situations in the coming months and years. All require companies to rethink how they prepare for and respond to cyber crises.

1 ATTACKS Timed to Maximize Pain

Sophisticated threat actors will increasingly time their attacks around critical business moments: earnings releases, major product launches, seasonal peaks, travel surges, logistics deadlines or regulatory milestones. The Canvas learning platform incident

The **WORST** Possible **MOMENT**

at the end of the 2025–2026 school year illustrates the logic: Attackers potentially targeted a “no fail” moment of the student and teacher platform, widely relied on in higher education.

This requires companies to shift in how they manage cybersecurity preparedness. Security monitoring and threat hunting should reflect the operational calendar, with systems hardened ahead of high-stakes periods. Cyber playbooks must account for incidents arriving at precisely the worst time.

If an attack lands during a sensitive period, the first question is whether workarounds to compromised



systems can sustain operations long enough to contain the incident. Organizations should establish clear pay or no-pay criteria in advance, based on a realistic cost analysis of disruption at critical moments. Whatever the ransom decision, it should be kept as quiet as possible. Publicizing a payment invites future targeting. Let people speculate.

2 EXPOSURE of Sensitive AI Training DATA

Organizations are often integrating AI tools into daily workflows faster than governance and cybersecurity controls can mature. Sensitive client, legal, health or personal data may therefore sit inside AI systems with insufficient safeguards, creating new opportunities for extortion and reputational damage. Threat actors may even contact the customers, clients or patients whose data has been compromised, pressuring the victim organization to pay a ransom to prevent further disclosure.

A crucial step that sounds obvious but is in fact challenging: Ensure your organization's cyber-

AI is making it easier for threat actors to time strikes for maximum disruption. Here are **FIVE SCENARIOS** for which boards must prepare.

security and privacy governance keeps pace with AI adoption. Set clear rules for what employees may enter into AI tools, and routinely take inventory of sensitive training data. Cyber playbooks should also include scenarios in which that data is exposed.

If an AI-training-data breach occurs, the critical question is which stakeholders are affected and how sensitive the exposed data is. As a general rule, stakeholders should hear about the incident from the company first, before a threat actor contacts them. Organizations should communicate clearly about the steps they are taking to investigate and lock down training data against further exposure.

3 DATA POISONING and Information Manipulation

As organizations rely more heavily on data-driven AI, threat actors may shift from stealing or encrypting data to corrupting it. In a data poisoning attack, malicious false information is inserted into AI training datasets, operational systems or knowledge repositories. The result can create an operational and reputational crisis in which the central question is what information can still be trusted.

Companies should institute processes to regularly test data integrity and maintain validated backups—steps they should understand and be able to communicate. They should also retain forensic expertise capable of identifying manipulation. The key is finding where the threat actor inserted carefully disguised errors. If faced with a data poisoning incident, the priority is to communicate clearly about why data can be trusted or, if it cannot yet be trusted, to lay out the remediation path the company is following to restore accuracy. Where feasible, work with forensics investigators to employ AI tools to help speed the investigation.

4 GLOBAL CYBER Outage

The world has not yet experienced a true cyber contagion event, where a backbone of the global network is crippled. But dependence on a small number of cloud providers, infrastructure operators and software platforms is increasing the risk of systemic disruption. The next major cyber event may not involve your company or its networks directly, but your operations may still be affected if a key vendor or supply-chain partner is debilitated.

Organizations should inventory the critical vendor systems whose failure would cripple essential business functions, and create business continuity plans and cyber playbooks that account for these kinds of situations. Before a real event forces

THE ADVANTAGE ATTACKERS GAIN FROM BETTER INTELLIGENCE CAN BE COUNTERED BY BETTER PREPARATION.

ADMIRAL MIKE ROGERS, a Brunswick Senior Advisor, retired from the US Navy in 2018 as a four-star admiral. He served simultaneously as Commander, US Cyber Command and Director, National Security Agency. **PRESTON GOLSON**, a Director, was formerly an analyst at the CIA and an aide to two Directors of National Intelligence. Rogers and Golson are based in Washington, DC.

the question, test critical operations that could be affected in degraded network environments.

If a global outage occurs, clearly communicate with customers and stakeholders about why systems are down and what workarounds exist. Resist the temptation to overpromise on restoration timelines. Honesty about what is known and what is unknown will do more for long-term trust than optimistic forecasts that prove wrong.

5 MULTI-VULNERABILITY Discovery

Powerful AI cybersecurity tools are making it dramatically easier to find software vulnerabilities. But they also mean companies can be overwhelmed by what they find. Using Claude Mythos Preview and other AI models, Mozilla shipped 423 Firefox bug fixes in April 2026, compared to anywhere between 17 and 76 in previous months. In such cases, knowing the extent of the problem can be an incident in itself, making it difficult to even prioritize major problems over minor ones. Previously, companies could not be held responsible for vulnerabilities they did not know about. With tools like Mythos, ignorance is no longer bliss.

Organizations should tighten their vulnerability disclosure policies in close coordination with cybersecurity, legal, operational and communications teams. They also need clear and defensible thresholds for what constitutes a critical vulnerability that warrants a public warning, even when a fix is not yet available. Companies should not wait for access to the most powerful discovery tools to begin the work of identifying the most serious vulnerabilities. Existing models can surface such problems today.

If vulnerabilities publicly emerge in large numbers, triage is the imperative: Identify what is critical, communicate clear remediation steps, and give customers and partners practical instructions for protecting themselves, perhaps on a dedicated microsite. After the immediate crisis has passed, communicate how the company is changing its policies and adopting more secure standards going forward.

What BOARDS and C-SUITES Should Do Now

AI is giving threat actors greater ability to understand not only how to attack a company, but when an attack will hurt most. Boards and senior executives now have the responsibility to know where those moments of maximum dependency lie, ensure cyber plans account for them, and make the hardest decisions before a crisis arrives.

The advantage attackers gain from better intelligence can be countered by better preparation. ♦