Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Elise Quevedo

The domino effect – can security and privacy practices keep pace?



Cybersecurity has once again become one of the most pressing topics in technology. Recent incidents involving NVIDIA, Fireworks AI, Notion, Uber, and Maersk have pushed the issue back into focus.

The digital economy depends on an extraordinary amount of information moving between companies, cloud platforms, software providers, and AI systems. Personal data, financial records, business documents, credentials, and private conversations rarely stay within one organisation's boundaries.

Although we have built an economy around sharing information online because connected systems make businesses faster and services more convenient, every connection creates another point where information can be accessed, copied, or exposed.

The recent wave of incidents suggests that our ability to connect systems has outpaced our ability to secure the complex networks behind them. Let's dive in.

Data no longer stays with the company you originally trusted

One of the most important changes in cybersecurity is the growth of the digital supply chain. When someone gives their information to a company, they often assume that company controls and protects the data directly.

In reality, the information can pass through a large network of technology providers. A business might rely on one company for cloud computing, another for AI infrastructure, another for payments, another for customer support, and several more for data analytics and internal software.

Recent incidents at Fireworks AI show how quickly a problem at one technology provider can affect other businesses. Fireworks AI disclosed multiple security incidents in October, and a later investigation found that customer account and billing information had been exposed. For a limited set of customers, the impact also extended to secrets, datasets, and incomplete model weights.

The company said a separate incident involving a third-party cloud provider allowed attackers to reach its development machines and caused additional customer data exposure.

> You can carefully choose which companies to trust, yet still have little visibility into the wider ecosystem of businesses handling your information

Notion, which used Fireworks AI for parts of its AI infrastructure, later confirmed that the incident affected some customer data.

Reports indicated that chat transcripts connected to Notion's AI Insights feature were among the exposed information. Notion estimated that fewer than 1% of its workspaces may have been affected and disconnected its systems from Fireworks during its response.

Uber provides another example of how this type of risk can spread. The company disclosed this week that an unauthorised party used compromised credentials at a service provider to access Uber data, with exposed information including US driver's licence details.

The incident reinforces that a company can invest heavily in its own security and still face a breach through an external provider with access to its systems or data.

It creates a difficult problem for consumers. You can carefully choose which companies to trust, yet still have little visibility into the wider ecosystem of businesses handling your information.

Privacy therefore involves more than deciding which data you are willing to share. It depends on how many other organisations gain access once the information enters a company's systems.

The digital attack surface keeps expanding

The second concern is the sheer scale of the modern attack surface. Businesses now connect more systems than ever before.

Cloud platforms now support critical operations, employees work across dozens of applications, and artificial intelligence tools sit alongside traditional business software. At the same time, organisations still run older systems built for a different security environment.

NVIDIA's recent security incident involving its Brev cloud development platform illustrates the risks associated with credentials and access. The company disclosed unauthorised activity on the platform between 4 October and 20 October.

The incident could have exposed SSH keys used to access customer virtual machines, although NVIDIA said it found no evidence that the keys were misused and rotated the affected credentials as part of its response.

The importance of incidents like this lies in what credentials represent. A password or access key does not need to contain valuable information itself. Its value comes from what it lets someone access.

In a highly connected cloud environment, compromised credentials can provide an attacker with a path into systems that contain far more sensitive data.

> As companies move more operations online, the range of assets worth attacking keeps growing

This is one reason identity and access management has become central to cybersecurity. The security challenge no longer involves only protecting a database from an outside attacker. Companies also need to control who, or what, can move between connected systems once they have gained access.

Another breach occurred at Maersk, a legacy system connected to the company's purchase of LF Logistics in 2022. The threat posed by outdated infrastructure is shown by a ransom demand and stolen data. Luckily, it did not interfere with its wider operations and only had an impact on a local area.

This issue will remain difficult for large organisations. Replacing legacy technology takes time, money, and careful planning. Yet every older system that remains connected can become a potential entry point.

The modern cybersecurity challenge is therefore partly a race between technological progress and the infrastructure companies already depend on. New AI systems, cloud services and connected devices continue to enter the workplace, while older technology remains in place behind them.

Attackers are also becoming more specialised. Fireworks said evidence from its investigation pointed to financially motivated activity linked to LLMJacking, where criminals access AI resources and sell or exploit the computing capacity.

Google's threat intelligence researchers have described fraudulent usage costs reaching more than $100,000 in a single day in some incidents, with cumulative losses at some organisations reaching $1 million before access was revoked.

The concern is that attackers can target access to computing power, AI models, cloud accounts, and other digital resources with financial value. As companies move more operations online, the range of assets worth attacking keeps growing.

Privacy is becoming more complicated in the age of AI

Cybersecurity and privacy overlap, but they

address different problems. Cybersecurity focuses on preventing unauthorised access. Privacy asks what information companies should collect, how they should use it, and how long they should keep it.

AI systems become more useful with context. People upload documents, share conversations, connect business accounts, and provide systems with information that helps generate more relevant results. Companies also send proprietary data to AI providers for training, analysis, and inference.

The recent Notion and Fireworks incident shows why this deserves closer attention. A conventional breach might expose names, email addresses, or account details. AI-related data can reveal something more detailed about how people work and communicate.

A chat transcript can contain internal business discussions, customer information, product plans, research, or personal concerns. Even when individual records cannot easily be linked to a specific person, the information itself can still be valuable.



AI-related data can reveal something more detailed about how people work and communicate

The more information we share with digital services, the more important data minimisation becomes. Companies need to ask whether they genuinely need every piece of information they collect and whether they need to keep it indefinitely.

Reducing unnecessary data storage does not eliminate cybersecurity risk, but it limits what attackers can access when a system is compromised.

Businesses also need stronger oversight of third-party providers. Vendor security reviews cannot become a one-time exercise completed when a contract is signed.

Companies need to understand what external providers can access, where sensitive information is stored, how credentials are managed, and what happens when a provider experiences a breach.

The Fireworks incidents show how a security problem at one company can become a privacy problem for several others.

Companies will become even more dependent on one another's technology

For us as individuals, the same principle applies on a smaller scale. Every connected account, AI tool, and application increases the amount of information stored about us online. We need clearer information about what companies collect and where it goes, while companies need to make those decisions easier to understand.

The recent incidents involving NVIDIA, Fireworks AI, Notion, Uber, and Maersk point to the same challenge. The digital world is more interconnected than ever, but accountability for security and privacy is fragmented across highly complex technology ecosystems.

> The challenge is whether security and privacy practices can keep pace

Companies should ask themselves whether they need to collect the data in the first place, how long they should retain it, and how many external organisations should have access to it.

Everything will continue moving online. AI will

become more integrated, and companies will become even more dependent on one another's technology.

The challenge is whether security and privacy practices can keep pace.