11TH Edition

2024 Data Breach Industry Forecast

experian

Contributors

Michael Bruemmer

Vice President, Global Data Breach Resolution

Michael Bruemmer is Vice President of Global Data Breach & Consumer Protection at Experian. The group is a leader helping businesses prepare for a data breach, manage consumer crisis response programs and mitigate consumer risk following incidents.

With more than 25 years in the industry, Michael brings a wealth of knowledge related to crisis response management from discovery to post-incident clean up. He has handled some of the nation's largest data breaches during his tenure with Experian and more than 60,000 to date. Michael has educated businesses of all sizes and sectors on pre-breach and breach response planning and delivery. This ranges from how to notify affected consumers, to call center set up and even how to implement identity theft protection services.

He is a respected speaker and presents to industry organizations across the country. He has provided insight to many trade and business media outlets including Dark Reading, IT Business, CIO, Info Security, Security Week, Health IT Security, Wall Street Journal, and American Banker among others. He has been a guest columnist for SecurityInfoWatch and has appeared on broadcast channels such as Fox Business.

He currently resides on the Ponemon Responsible Information Management (RIM) Board and NetDiligence Advisory Board.

He holds a Bachelor of Arts in Labor Economics from the University of Wisconsin-Madison.

Jim Steven

Head of Crisis & Data Response Services, UK

Jim Steven is Head of Crisis & Data Breach Response Services for Experian UK, building on the knowledge, experience and success of Experian's global data breach resolution offering.

His team works with businesses to help them manage and resource mass consumer crisis responses, including customer notification, contact center and credit/identity monitoring services for customers/employees affected by a crisis event. They also support clients in preparing and practicing readiness plans for potential incidents to mitigate the impact and speed of recovery.

Prior to joining Experian, Jim worked in the security and risk management industry providing expertise in security risk management solutions, travel risk management, aviation security and corporate security for some of the world's largest security companies.

Executive Summary

After slowing down in 2022, this year looks to be record-setting for total data breaches. According to the Identity Theft Resource Center[1], there are already 2,116 data compromises as of Q3, surpassing last year's total. Notably, Experian has supported 2,294 data breaches alone pointing to possible under-reporting, so the numbers could be much higher. According to our internal analytics, more than 70 million consumers globally were impacted by a data breach from our client base in 2023—up 30 percent since last year.

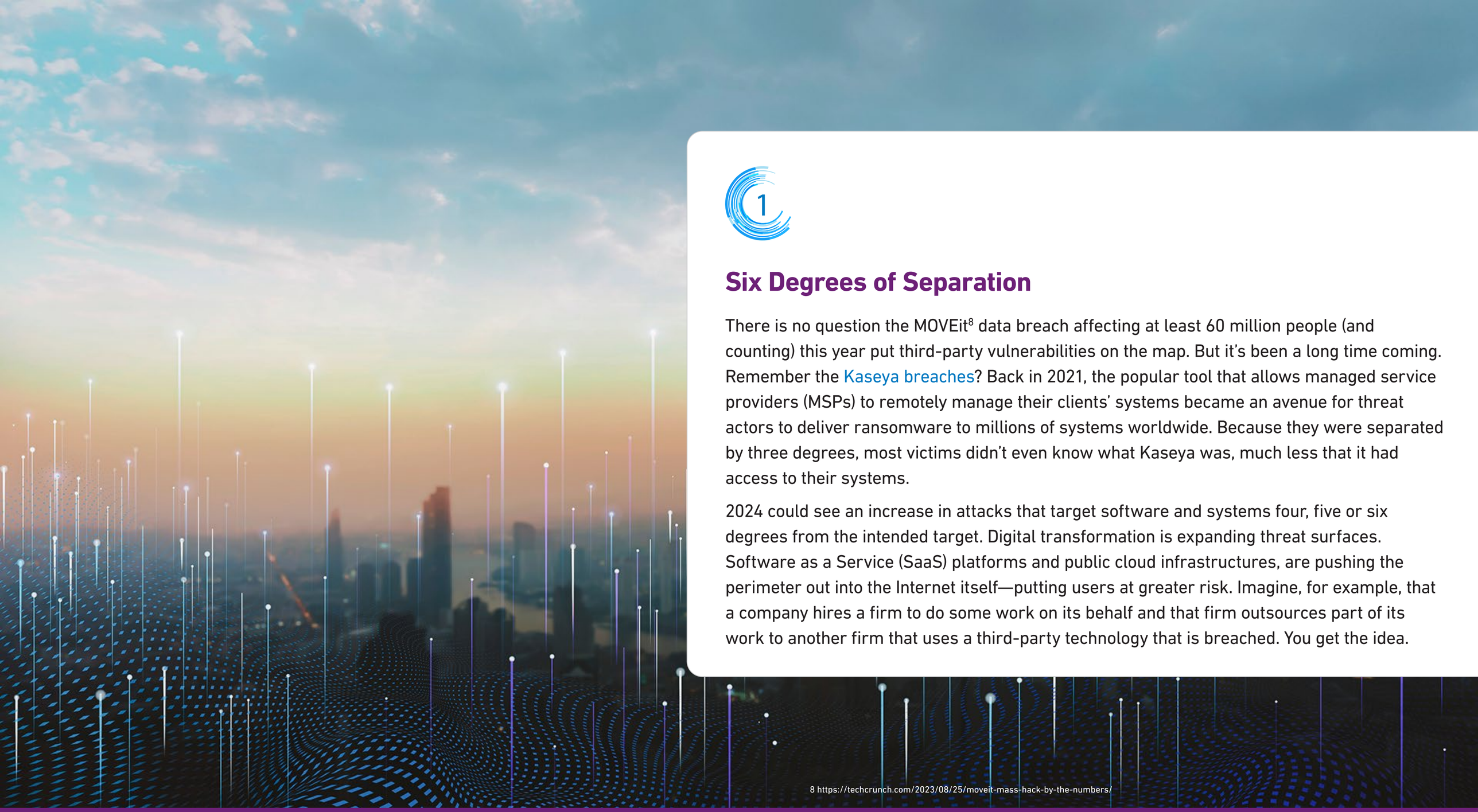
It only takes one "success" story for hackers to move the year into the record books. In 2023, we saw two large data breaches (DarkBeam[2] and MOVEit[3]) that reportedly affected more than three billion records combined to lead the way.

A few of our predictions for this year were realized showing there is no safe "space" from bad actors as there were hacks on satellites, including reports[4] by the Ukraine State Security Service (SBU) that Russian spy agencies targeted Starlink with custom malware. We talked about artificial intelligence last year, and that has certainly been a hot topic among many industries on ways to harness it. Hackers are no different – they want to leverage it too. Earlier this year, it was reported in a news story that a chatbot's API was hacked[5] pushing out malware code and the Federal Bureau of Investigation warned[6] that hackers are running wild deploying AI tools.

In our 11th annual Data Breach Industry Forecast, we looked more broadly than ever before at trends and data on a global scale as data breaches have no borders. This, along with the fact that nation-state-sponsored gangs and attacks are becoming increasingly more strategic and purposeful due to political conflicts or interests, made it fitting to expand our lens. Our predictions come from Experian's long history of helping companies navigate breaches over the past 21 years. Here's where we expect to see some hard to believe, but possible developments in the world of data security incidents in 2024.

The Data Breach Industry Forecast is Experian's attempt at looking into our crystal ball and providing cybersecurity predictions for what may lie ahead. The predictions are not guaranteed, should not be relied on as formal advice and are intended for educational purposes only.

1 https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/
2 https://www.databreaches.net/more-than-3-8-billion-records-exposed-in-darkbeam-data-leak/
3 https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/
4 https://www.telegraph.co.uk/business/2023/08/12/russian-spy-agencies-targeting-elon-musk-starlink-malware/
5 https://www.digitaltrends.com/computing/hackers-using-ai-chatgpt-to-create-malware/
6 https://www.digitaltrends.com/computing/hackers-using-ai-chatgpt-to-create-malware/



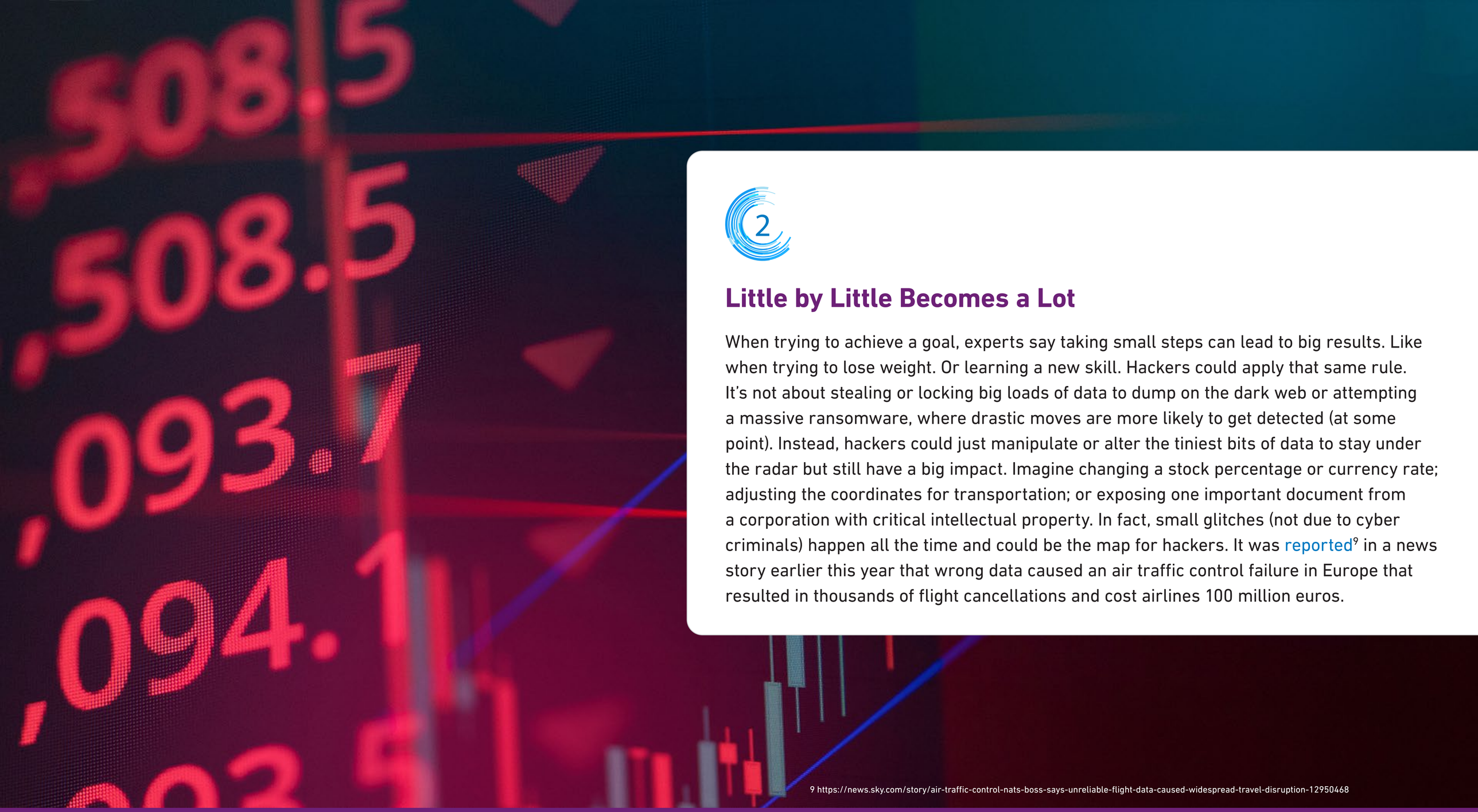
1

Six Degrees of Separation

There is no question the MOVEit[8] data breach affecting at least 60 million people (and counting) this year put third-party vulnerabilities on the map. But it's been a long time coming. Remember the Kaseya breaches? Back in 2021, the popular tool that allows managed service providers (MSPs) to remotely manage their clients' systems became an avenue for threat actors to deliver ransomware to millions of systems worldwide. Because they were separated by three degrees, most victims didn't even know what Kaseya was, much less that it had access to their systems.

2024 could see an increase in attacks that target software and systems four, five or six degrees from the intended target. Digital transformation is expanding threat surfaces. Software as a Service (SaaS) platforms and public cloud infrastructures, are pushing the perimeter out into the Internet itself—putting users at greater risk. Imagine, for example, that a company hires a firm to do some work on its behalf and that firm outsources part of its work to another firm that uses a third-party technology that is breached. You get the idea.

8 https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/

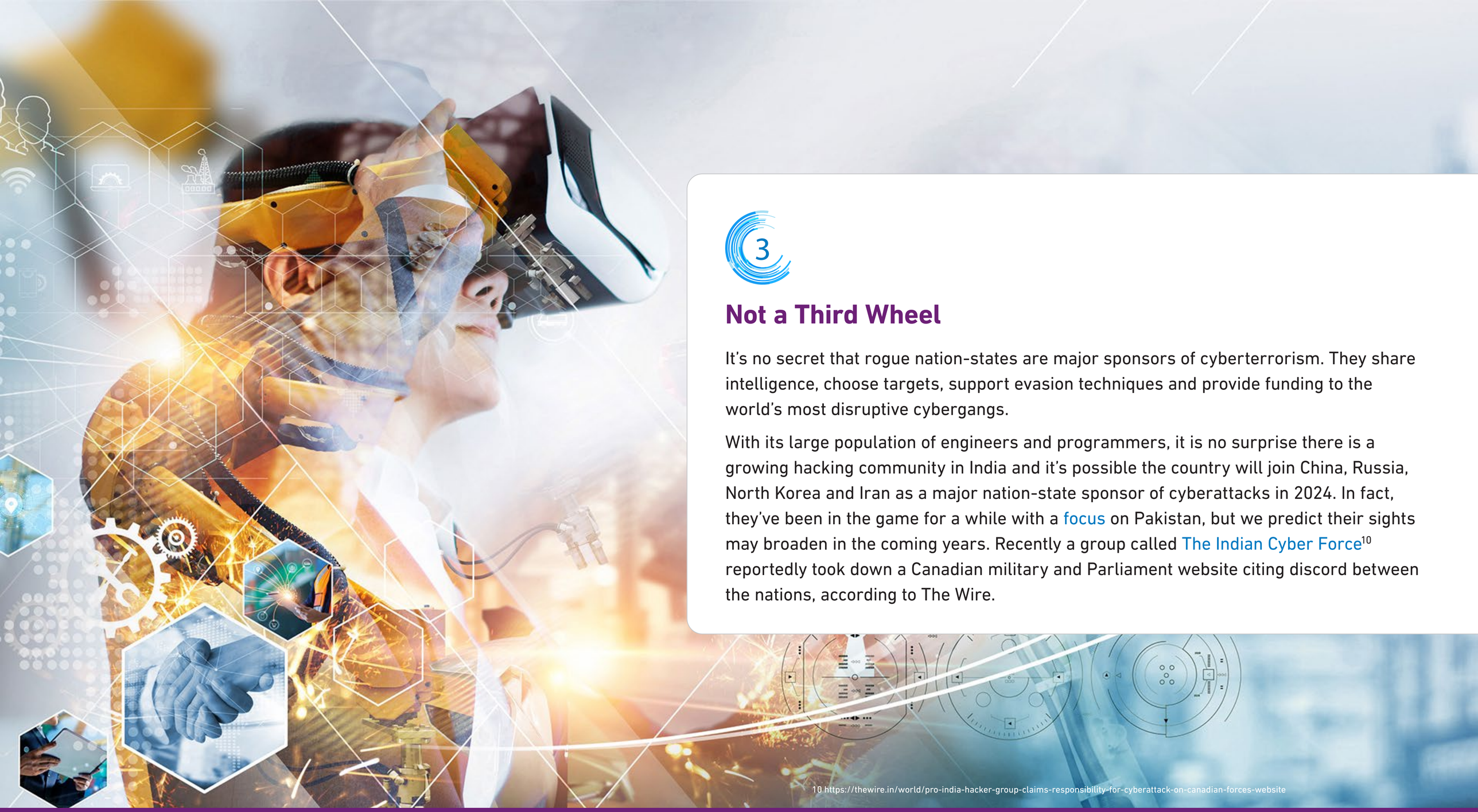


2

Little by Little Becomes a Lot

When trying to achieve a goal, experts say taking small steps can lead to big results. Like when trying to lose weight. Or learning a new skill. Hackers could apply that same rule. It's not about stealing or locking big loads of data to dump on the dark web or attempting a massive ransomware, where drastic moves are more likely to get detected (at some point). Instead, hackers could just manipulate or alter the tiniest bits of data to stay under the radar but still have a big impact. Imagine changing a stock percentage or currency rate; adjusting the coordinates for transportation; or exposing one important document from a corporation with critical intellectual property. In fact, small glitches (not due to cyber criminals) happen all the time and could be the map for hackers. It was reported[9] in a news story earlier this year that wrong data caused an air traffic control failure in Europe that resulted in thousands of flight cancellations and cost airlines 100 million euros.

9 https://news.sky.com/story/air-traffic-control-nats-boss-says-unreliable-flight-data-caused-widespread-travel-disruption-12950468



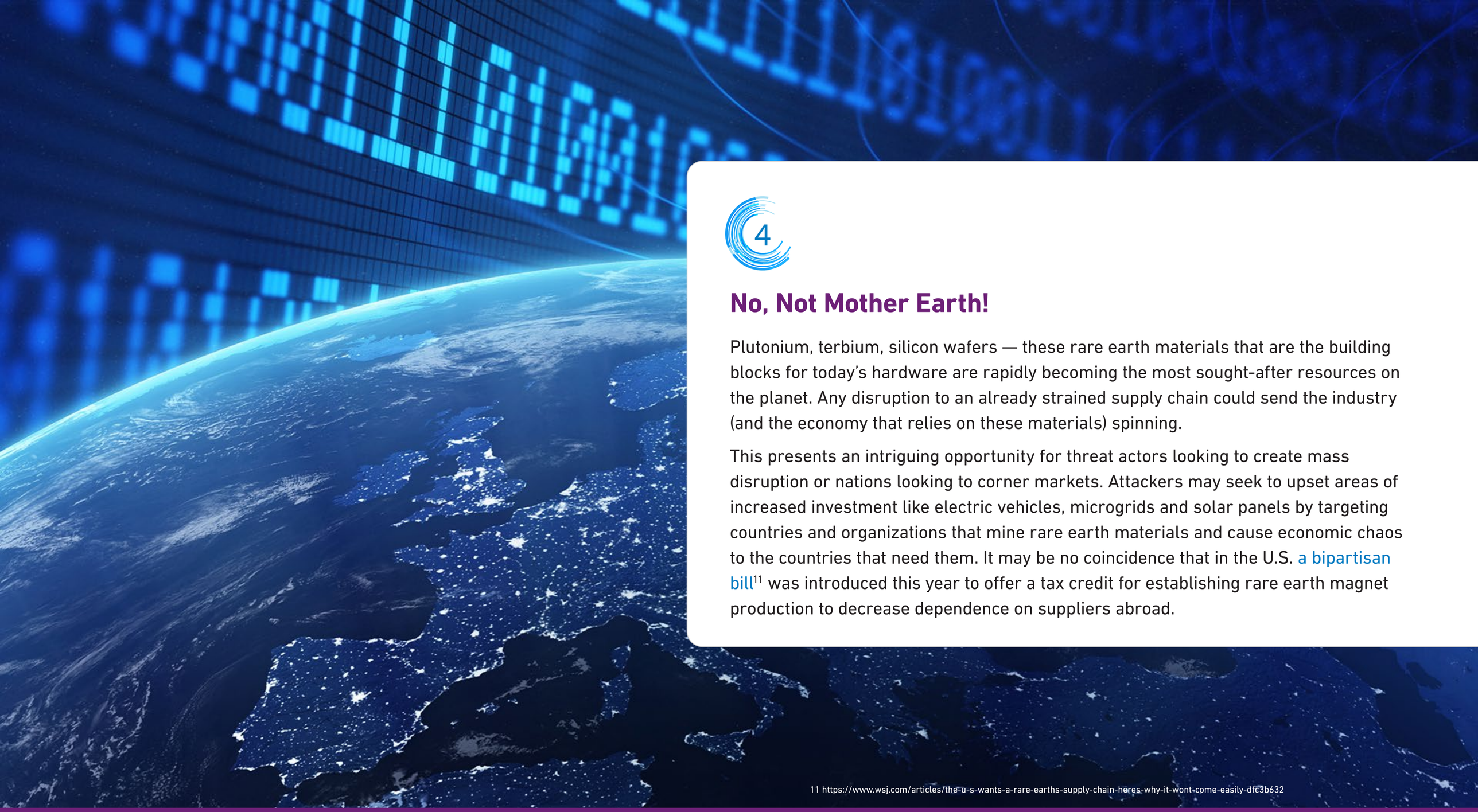
3

Not a Third Wheel

It's no secret that rogue nation-states are major sponsors of cyberterrorism. They share intelligence, choose targets, support evasion techniques and provide funding to the world's most disruptive cybergangs.

With its large population of engineers and programmers, it is no surprise there is a growing hacking community in India and it's possible the country will join China, Russia, North Korea and Iran as a major nation-state sponsor of cyberattacks in 2024. In fact, they've been in the game for a while with a focus on Pakistan, but we predict their sights may broaden in the coming years. Recently a group called The Indian Cyber Force[10] reportedly took down a Canadian military and Parliament website citing discord between the nations, according to The Wire.

10 https://thewire.in/world/pro-india-hacker-group-claims-responsibility-for-cyberattack-on-canadian-forces-website



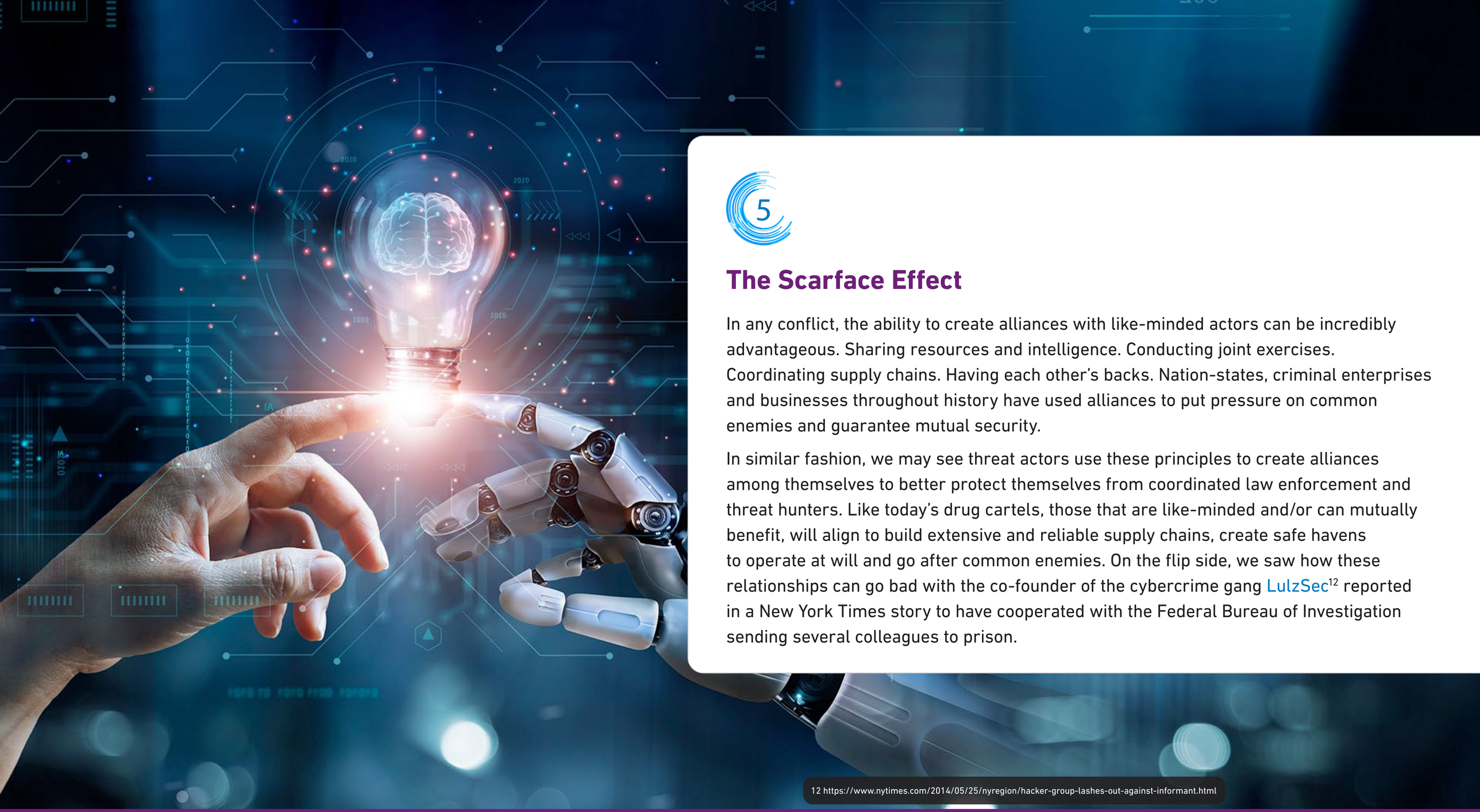
4

No, Not Mother Earth!

Plutonium, terbium, silicon wafers — these rare earth materials that are the building blocks for today's hardware are rapidly becoming the most sought-after resources on the planet. Any disruption to an already strained supply chain could send the industry (and the economy that relies on these materials) spinning.

This presents an intriguing opportunity for threat actors looking to create mass disruption or nations looking to corner markets. Attackers may seek to upset areas of increased investment like electric vehicles, microgrids and solar panels by targeting countries and organizations that mine rare earth materials and cause economic chaos to the countries that need them. It may be no coincidence that in the U.S. a bipartisan bill[11] was introduced this year to offer a tax credit for establishing rare earth magnet production to decrease dependence on suppliers abroad.

11 https://www.wsj.com/articles/the-u-s-wants-a-rare-earths-supply-chain-heres-why-it-wont-come-easily-dfc3b632



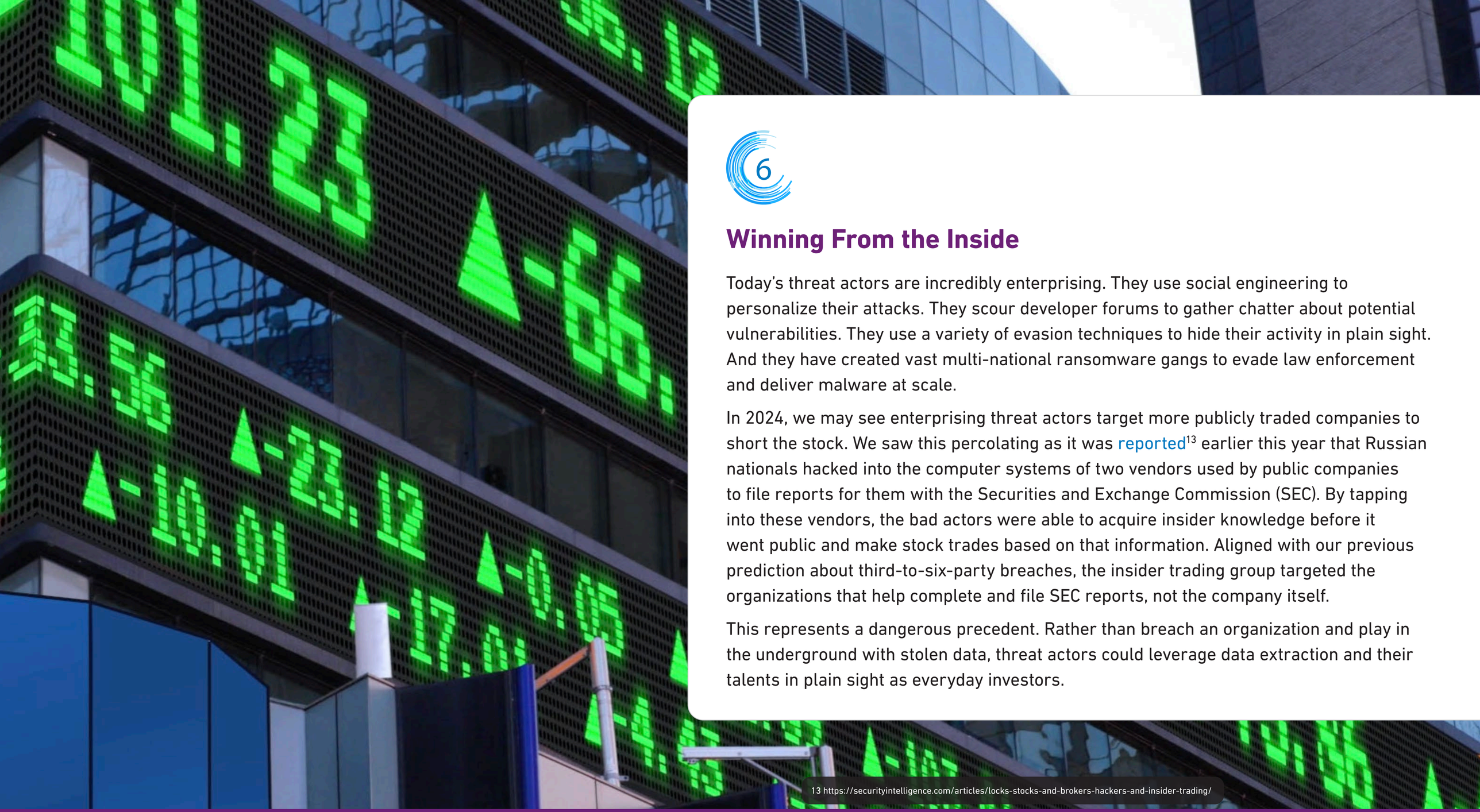
5

The Scarface Effect

In any conflict, the ability to create alliances with like-minded actors can be incredibly advantageous. Sharing resources and intelligence. Conducting joint exercises. Coordinating supply chains. Having each other's backs. Nation-states, criminal enterprises and businesses throughout history have used alliances to put pressure on common enemies and guarantee mutual security.

In similar fashion, we may see threat actors use these principles to create alliances among themselves to better protect themselves from coordinated law enforcement and threat hunters. Like today's drug cartels, those that are like-minded and/or can mutually benefit, will align to build extensive and reliable supply chains, create safe havens to operate at will and go after common enemies. On the flip side, we saw how these relationships can go bad with the co-founder of the cybercrime gang LulzSec[12] reported in a New York Times story to have cooperated with the Federal Bureau of Investigation sending several colleagues to prison.

12 https://www.nytimes.com/2014/05/25/nyregion/hacker-group-lashes-out-against-informant.html



6

Winning From the Inside

Today's threat actors are incredibly enterprising. They use social engineering to personalize their attacks. They scour developer forums to gather chatter about potential vulnerabilities. They use a variety of evasion techniques to hide their activity in plain sight. And they have created vast multi-national ransomware gangs to evade law enforcement and deliver malware at scale.

In 2024, we may see enterprising threat actors target more publicly traded companies to short the stock. We saw this percolating as it was reported[13] earlier this year that Russian nationals hacked into the computer systems of two vendors used by public companies to file reports for them with the Securities and Exchange Commission (SEC). By tapping into these vendors, the bad actors were able to acquire insider knowledge before it went public and make stock trades based on that information. Aligned with our previous prediction about third-to-six-party breaches, the insider trading group targeted the organizations that help complete and file SEC reports, not the company itself.

This represents a dangerous precedent. Rather than breach an organization and play in the underground with stolen data, threat actors could leverage data extraction and their talents in plain sight as everyday investors.

13 https://securityintelligence.com/articles/locks-stocks-and-brokers-hackers-and-insider-trading/

Experian® Data Breach Resolution by the numbers

2,294
Total client data breaches in 2023

68,505,814
Consumers impacted in 2023

7
Total mega breaches in 2023

Total breaches by sector:

- 38% Healthcare
- 21% Financial Services
- 16% Public Sector
- 12% Retail
- 10% Education

Coverage:

100+ Countries

Top 5 countries hit hardest:

U.S.
U.K.
Canada
Australia
Mexico

Consumers impacted:

22% Children
78% Adults

Better outcomes, unmatched value

Count on Experian Data Breach resolution for the partnership, solutions and performance to create the best possible outcome. Gain control and confidence with the value that only Experian Partner Solutions can provide.

We are your trusted partner and the leader in the industry

21+ years

managing crisis and breach programs[14]

30 million+

crisis-related notifications delivered each year[14]

65,000+

incidents served[14]

16%

fewer breach events experienced for Reserved Response clients[14]

Here are some general stats (non-Experian) you may be interested in:

- **54% of organizations were breached through third-parties over a 12-month period.**
  Source: VentureBeat.2022. Report: 54% of organizations breached through third-parties in the last 12 months.
- **Cybercrime cost 8 Trillion Dollars in 2023 or $15.2M per minute**
  Source: Esentire, 2022 Official Cybercrime Report. 2022
- **60% of consumers are less likely to work with a brand that has suffered a data breach**
  Source: Business Wire, New Data From ThreatX Reveals 90% of Consumers are Concerned Poor Vendor Security Will Negatively Impact Their Lives in 2023, March 2023.
- **82% of breaches involve the human element**
  Source: Verizon, 2022 Data Breach Investigations Report

14 Experian Data, June 2023