MOODY'S RATINGS

SECTOR IN-DEPTH
1 April 2026

Send Your Feedback

TABLE OF CONTENTS

Contacts

Sanja Nedic +33.6.8393.3742
AVP-Data Scientist
sanja.nedic@moodys.com

Yoni Katz +1.212.553.3492
Lead Cyber Credit Risk Associate
yoni.katz@moodys.com

Leroy Terrelonge +33.1.5330.5989
VP-Sr Credit Officer
leroy.terrelonge@moodys.com

Lesley Ritter +1.212.553.1607
SVP-Cyber Credit Risk
lesley.ritter@moodys.com

Fabian Astic +1.212.553.6814
Managing Director, Global Head of Digital Economy
fabian.astic@moodys.com

CLIENT SERVICES

Americas 1-212-553-1653
Asia Pacific 852-3551-3077
Japan 81-3-5408-4100
EMEA 44-20-7772-5454

Cybersecurity – Global

Risks posed by unpatched software flaws vary by industry and region

Summary

Cyberattacks can undermine an organization's creditworthiness, hitting its revenues and increasing costs. In this report, we focus on one of the leading entry points for cyberattacks: exploitation of software vulnerabilities in IT products. Software vulnerabilities, often called bugs, are one of the easiest ways for criminals to penetrate an organization's internal digital network. Left unpatched, they pose a large and growing risk of cyberattacks for companies and organizations. We analyzed two years of data showing exposure of around 9,500 issuers to unpatched vulnerabilities. We find that risks vary according to an organization's digital footprint, but also to the industry they are in and the part of the world they operate in.

» **Software bugs present a growing cybersecurity risk.** In 2025, some 60% of organizations in our analysis had at least one externally observable known exploited vulnerability (KEV) in their networks. KEVs are software vulnerabilities confirmed by the US Cybersecurity and Infrastructure Security Agency (CISA) to have been used by cybercriminals to illegally penetrate a network. On average, close to 40% of issuers in any given month had an unpatched KEV that was older than 45 days - the time it typically takes attackers to exploit such vulnerabilities. More than a quarter had at least one that remained externally observable for over a year.

» **Exposure varies sharply across regions and industries.** Issuers in Japan and Korea are more likely to have old unpatched KEVs in their networks than peers in North America and Western Europe, while sectors such as education, telecommunications and technology have a higher prevalence than banking and utilities. The differences likely reflect variations in technology products, remediation constraints and regulations.

» **Exposure to unpatched KEVs rises with digital footprint size.** Organizations with a larger Internet-facing footprint[1] show a higher prevalence of unpatched KEVs. In our analysis, 78% of issuers in the top 10% of those with critical Internet-facing IT systems were affected by old unpatched KEVs, compared with 7.2% in the bottom 10%. Even among organizations with comparable digital footprints, exposure to unpatched KEVs varies considerably according to location and industry, suggesting that operating context shapes vulnerability beyond attack surface alone.

» **Patching outcomes vary.** Organizations fix KEVs more quickly than other software flaws, but not quickly enough to outpace attackers. KEVs known to have led to ransomware attacks are addressed fastest. Median patching times differ materially by sector and region, with some high-exposure sectors, such as telecommunications and education, slower to remediate than peers. At the sector level, exposure to +45-day KEVs is associated with a higher prevalence of subsequent cyber incidents.

Software bugs present a growing cybersecurity risk

The rising number of cybersecurity incidents affects the creditworthiness of our rated issuers by causing business disruption and by running up heavy remediation and legal costs. Many of these incidents begin with attackers exploiting weaknesses in widely used business software to gain access to corporate systems. These software flaws are difficult to eliminate quickly and completely, often leaving organizations exposed for extended periods.

Software vulnerabilities are a common entry point for attackers

Bugs in software consistently rank among the leading ways attackers gain entry into a victim's network. The 2025 Data Breach Investigations Report from US telecommunications firm Verizon Communications Inc. (Baa1 stable) found that exploitation of software flaws accounted for 20% of confirmed breaches, second only to the use of compromised sign-in credentials. In espionage-motivated attacks, they served as the access point in a striking 70% of cases. Similarly, Palo Alto Networks' Unit 42, a cybersecurity consulting and threat intelligence organization, reports that exploitation of software flaws and phishing were the leading entry points for cyberattackers in 2025.

Software bugs are easy targets for criminals. When high impact vulnerabilities emerge in Internet-facing software, attackers quickly automate Internet-wide scanning to identify and exploit vulnerable systems, often before organizations can patch them. As advances in AI shorten the gap between vulnerability disclosure and active misuse, the likelihood of unpatched systems being compromised is rising. A survey of more than 100 CEOs across industries and regions by the World Economic Forum shows that leaders view the exploitation of software vulnerabilities as one of their top three cyber risk concerns.

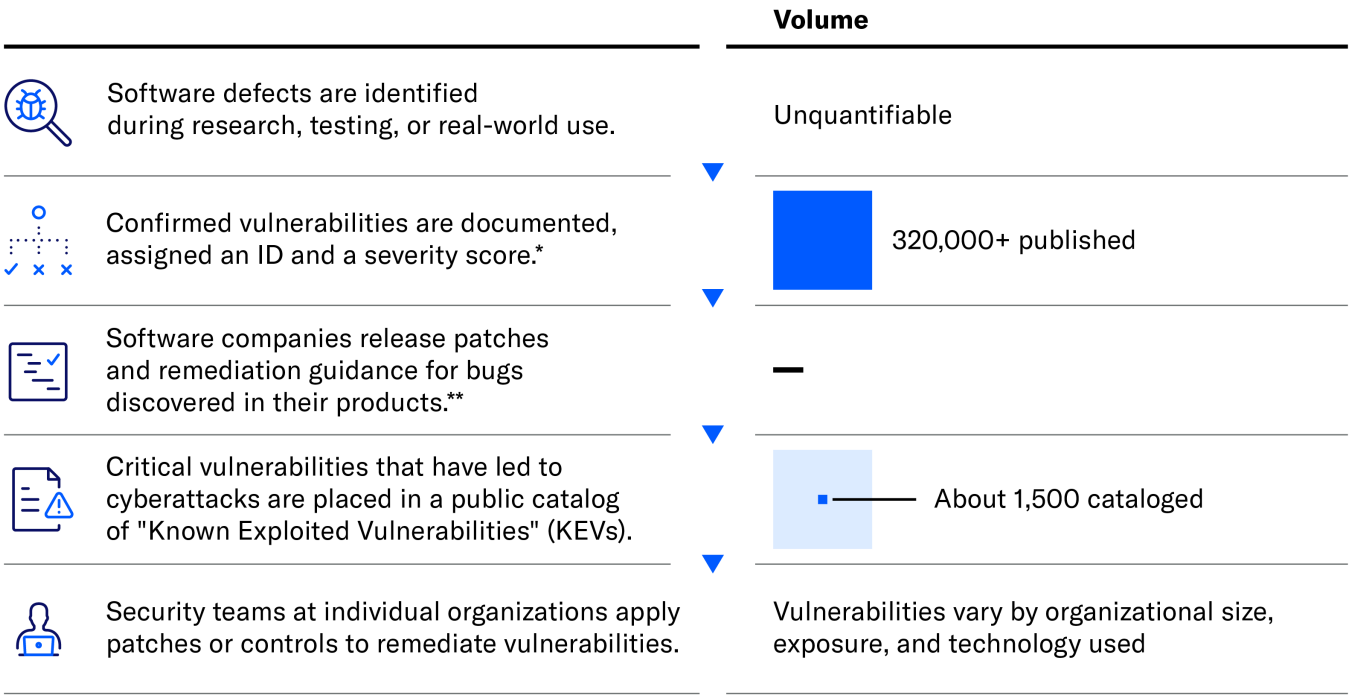
A small subset of disclosed vulnerabilities drives real-world attacks

Vast numbers of software defects are uncovered each year by security researchers, software vendors, bug bounty participants, threat actors and, increasingly, AI-powered automated tools (Exhibit 1).

Since 1999, the Common Vulnerabilities and Exposures (CVE) program, maintained by The MITRE Corporation, a non profit organization, has provided a catalog of publicly disclosed software vulnerabilities. By March 2026, this registry had expanded to more than 320,000 entries, with nearly 48,000 new vulnerabilities added in 2025 alone - equivalent to 4,000 new disclosures a month.

Only a fraction of these documented vulnerabilities will be used in real-world attacks. The US Cybersecurity and Infrastructure Security Agency (CISA) tracks Known Exploited Vulnerabilities (KEVs) based on credible evidence from incident response, threat intelligence or observed attacks. By flagging those with confirmed real-world exploitation, the KEV catalog helps companies prioritize the bugs that pose the most immediate risk. In February 2026, the catalog included some 1,500 entries, with an average of 20 new KEVs added each month in 2025. Some 20% are flagged as having been used in ransomware campaigns, which are typically very disruptive for the victim and so among the most damaging for credit quality.

Exhibit 1
Tens of thousands of software flaws are discovered each year
Only a small subset are used in cyberattacks



*CVE Numbering Authorities (CNAs) assign IDs; MITRE operates the CVE program; NIST's National Vulnerability Database (NVD) provides scores and additional data. ** While the real-world exploits may occur before a patch is released, the KEV catalog includes only vulnerabilities that carry clear remediation guidelines.
Sources: Moody's Ratings, MITRE, CISA

The most serious weaknesses cluster around a small group of widely used software providers

Entries in the KEV catalog are disproportionately concentrated among vendors whose products are widely deployed across enterprise IT environments. Large platform and infrastructure providers such as Microsoft Corporation (which accounts for close to a quarter of all KEVs) (Aaa stable), Apple Inc. (Aaa stable), Cisco Systems, Inc. (A1 stable), Adobe Inc. (A1 stable), and Google (Alphabet Inc., Aa2 stable), have long dominated the catalog, reflecting the wide use of their software across operating systems, browsers and foundational products. At the same time, vulnerabilities affecting network edge and secure access infrastructure feature prominently among newly cataloged KEVs, with cybersecurity and IT infrastructure companies such as Fortinet, Inc. (Baa1 positive) and Ivanti Software, Inc. (Caa1 stable) appearing more frequently as organizations expose more access infrastructure to the public internet.

The concentration does not imply that those vendors are uniquely insecure. Rather, it reflects factors that shape attacker incentives or detection outcomes. These include:

» **Scale and ubiquity:** Vendors with large user bases and deep enterprise integration are attractive targets for attackers because a single exploitable flaw can yield access to large numbers of organizations, offering a high return on investment.

» **Perimeter placement:** KEVs disproportionately affect virtual private networks, firewalls, gateways and identity infrastructure. These systems are typically Internet-facing and in many cases exploitation can occur with limited attacker effort and without requiring prior authentication or user interaction.

» **Visibility:** Large vendors are more closely monitored by researchers, governments and security teams, increasing the chance that exploitation of bugs in their software is detected.

Known exploited vulnerabilities are pervasive across our rated universe

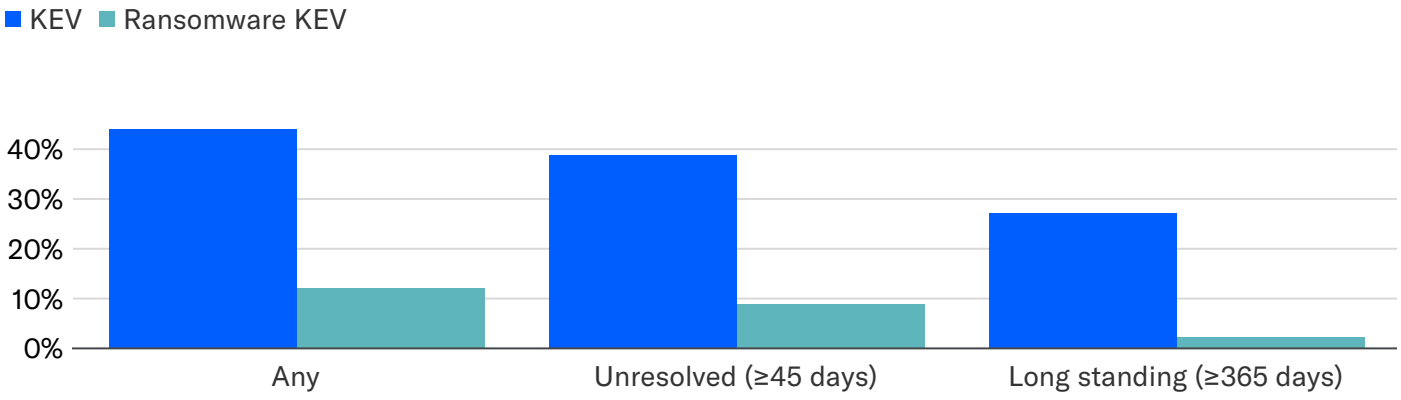
We have measured the prevalence of high-risk software vulnerabilities at roughly 9,500 issuers worldwide[2], across all rated industries. Our analysis spans two years and uses data from our affiliate Bitsight Technologies, a provider of cybersecurity ratings and analytics.

Bitsight scans the Internet to identify weaknesses that attackers can exploit. These are the systems cybercriminals target first. This allows tracking of a considerable share of the most dangerous, widely exploited vulnerabilities identified by CISA (as of February 2026, Bitsight tracks roughly 35% of KEVs), as well as tens of thousands of other known software flaws that pose a broad and significant risk.

Combining Bitsight data with our own, we found that in 2025 roughly 60% of the issuers in scope had at least one known vulnerability that had been confirmed by CISA to have been used in a cyberattack. In a typical month, close to 40% had an unresolved KEV on their networks observable for at least 45 days. The 45-day threshold exceeds the typical 44 days that attackers take to exploit newly disclosed software weaknesses. More than a quarter had at least one outstanding KEV that remained unpatched for over a year (Exhibit 2).

CISA recommends remediation within 21 days for most KEVs, and shorter timelines for those linked to ransomware activity, among the most disruptive attacks for an organization to deal with. Close to 10% of issuers had a vulnerability known to have been used in ransomware campaigns that was older than 45 days. Among organizations with at least one known exploited vulnerability, exposure was often not limited to a single instance - the median issuer had 10[3] such vulnerabilities, while a quarter had more than 34 instances, indicating that KEVs frequently persist across multiple systems.

Exhibit 2
KEV prevalence by type and duration of exposure
Share of issuers with a known exploited vulnerability in an average month in 2025



Sources: Moody's Ratings, Bitsight Technologies

Exposure varies sharply across regions and industries

Regional differences in exposure to KEVs older than 45 days are pronounced (Exhibit 3). In our analysis, we grouped advanced economy issuers into distinct regions to reflect differences in cyber governance and regulatory environments. They are: **North America** (US and Canada); **EU+** (advanced economies in the EU, Iceland, Liechtenstein, Norway, and Switzerland); **UK**; **Japan**; **Korea**; and **Asia advanced economies** (Hong Kong SAR, China, Macao SAR, China, Singapore, and Taiwan, China).

Among advanced economies, issuers in **Japan** and **Korea** are worst positioned with more than half of rated issuers affected by unresolved KEVs, observed for at least 45 days, driven by heavy exposure among non-financial corporates.

By contrast, **North America**, the **UK**, and **EU+** show lower prevalence, particularly among financial institutions, where +45-day KEVs were identified in the networks of roughly one third of issuers in an average month in 2025.

Australia and **New Zealand** are best placed across both non-financial corporates and financial institutions. Australia's lower exposure is consistent with strong regulatory coordination, including prescriptive financial-sector oversight by the Council of Financial Regulators

(CFR) and a centralized national approach to information-sharing and cyber-incident response led by the Australian Cyber Security Centre (ACSC). This coordination likely supports faster identification and remediation of software weaknesses.

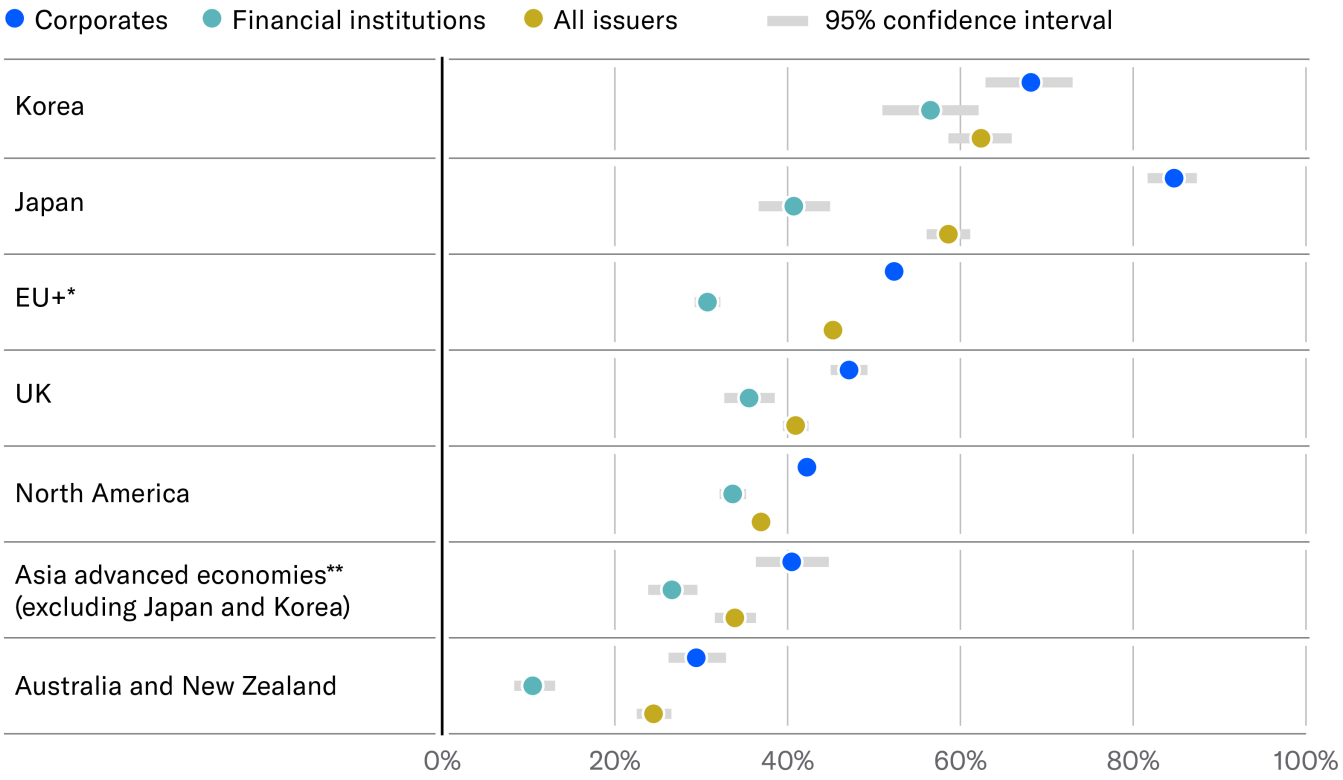
Across advanced economies, **non-financial companies** are consistently more exposed than **financial institutions**, although the size of this gap varies by region. The lower prevalence among financial institutions is consistent with the sector operating under more prescriptive cyber risk supervision and their more sophisticated cyber defense practices than most other corporates.

Japan shows a particularly large gap between non-financial corporates and financial institutions, with 85% of non-financial firms affected, compared with 41% of financial institutions. This difference likely reflects slower modernization among non-financial corporates, which remain burdened by legacy systems, while financial institutions operate under more formal, sector-specific cyber expectations.

Exhibit 3

Exposure to unresolved software weaknesses differs across regions

Average monthly share of advanced economy issuers with KEVs observed for at least 45 days during 2025, by region and issuer type



*EU+ includes issuers in advanced economies in the EU, Iceland, Liechtenstein, Norway, and Switzerland; **Asia advanced economies include issuers based in Hong Kong SAR, China, Macao SAR, China, Singapore, and Taiwan, China.

Sources: Moody's Ratings, Bitsight Technologies

Our analysis also shows wide variations sector by sector

Exposure to unresolved KEVs also varies widely across sectors (Exhibit 4).

Educational institutions, including universities and colleges, exhibit the highest prevalence, followed by **telecommunications companies**, **media & entertainment firms**, and **technology hardware makers**, where, across 2025, monthly exposure levels exceeded 60% of issuers.

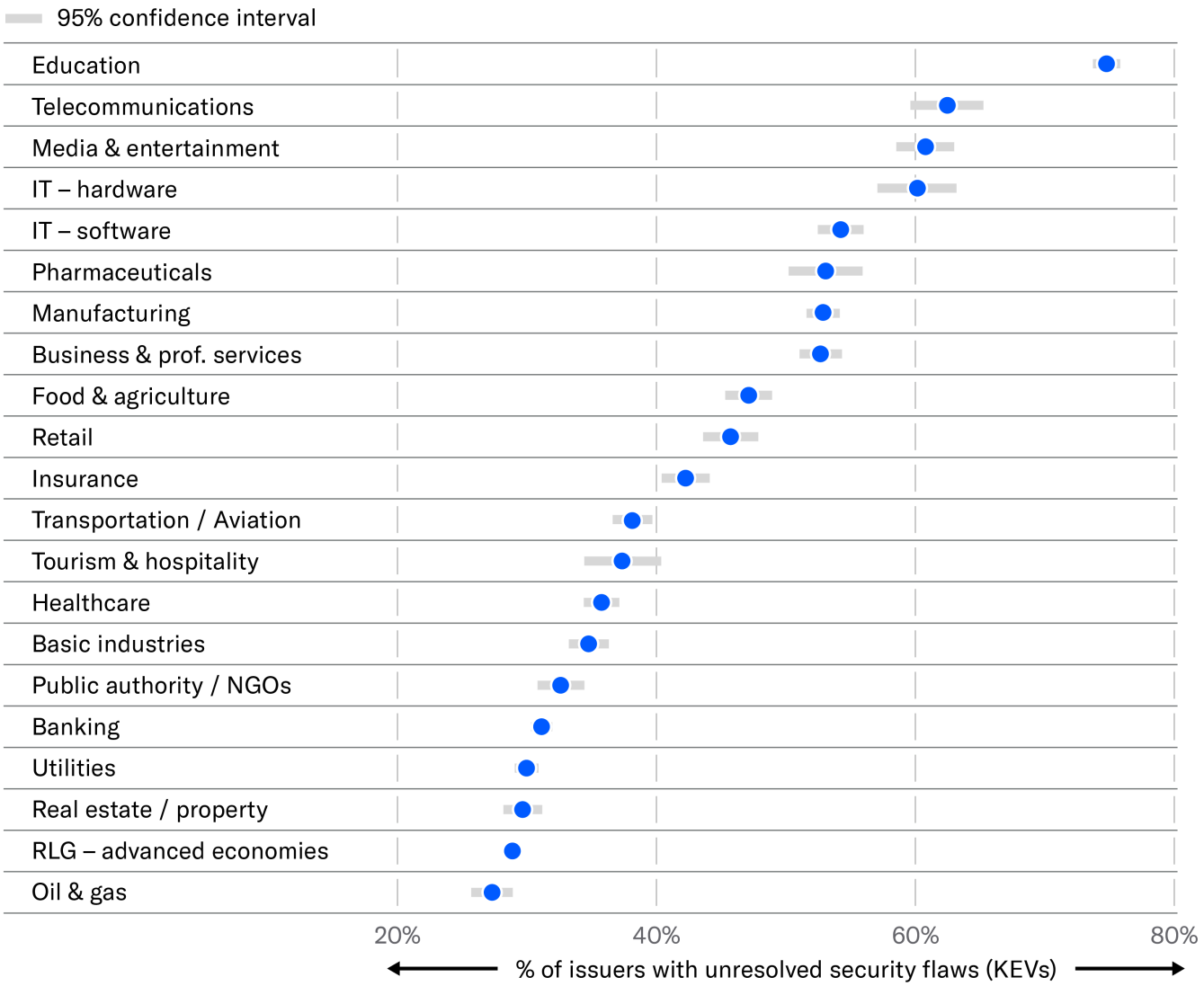
In part, this reflects the scale and complexity of these sectors' Internet exposure. Their digital footprints tend to be larger and more diverse than in many other industries, sometimes combining institutional infrastructure with customer, student, or third-party systems.

This increases the number of externally observable vulnerabilities. While data clearly linked to external users is excluded from our analysis when identified, separating user-controlled and issuer-controlled systems remains more challenging in some sectors. For example, telecommunications networks typically have clearer system boundaries, making this separation relatively easy, whereas educational institutions often operate more mixed environments.

Exhibit 4

Exposure to unresolved software weaknesses differs across sectors

Average monthly share of issuers with KEVs observed for at least 45 days during 2025, by sector



Sources: Moody's Ratings, Bitsight Technologies

By contrast, at **oil & gas companies**, **utilities**, **real estate firms**, **banks** and **regional and local governments (RLG) in advanced economies,** fewer than a third of issuers are exposed.

Beyond the scale of Internet-exposed digital footprints, these differences likely reflect variation in regulatory and institutional constraints, technology adoption and complexity, as well as constraints on remediation, including reliance on legacy systems and differences in patching practices. For example, the US National Institute of Standards and Technology (NIST), a federal agency that develops cybersecurity standards, among other things, notes that patching in operational-technology and industrial-control-system

environments, like manufacturing and industrial production lines, is often slower. This is because updates require extensive testing, must be coordinated with maintenance windows, can interrupt physical processes or production and may even be unavailable for older systems.

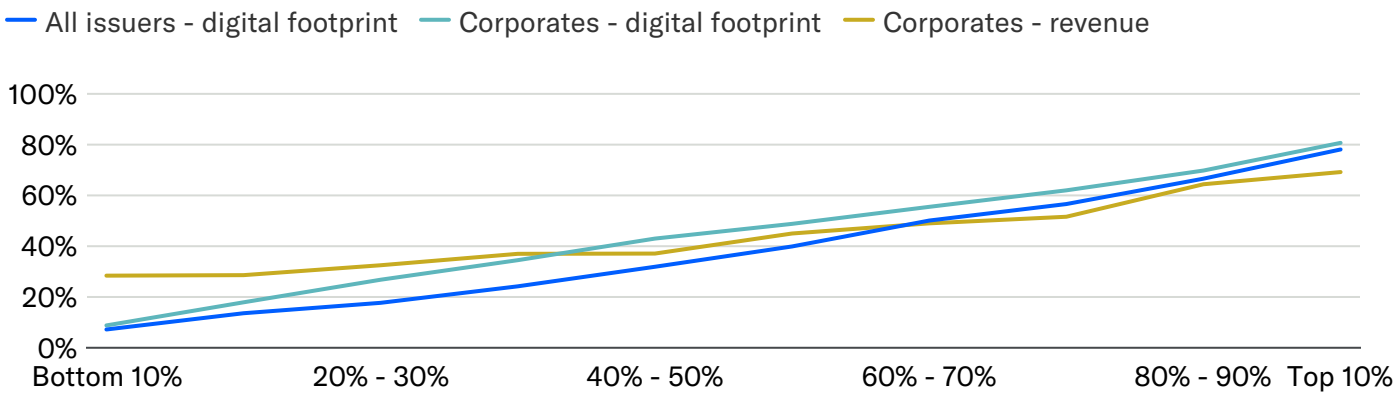
Exposure to unpatched KEVs rises with digital footprint size

Unsurprisingly, exposure to KEVs increases sharply with the size of an issuer's externally facing digital footprint[4]. In an average month, nearly 80% of issuers with the largest Internet-facing footprints exhibit at least one KEV, unpatched for at least 45 days, compared with fewer than 10% among issuers with the smallest footprints (Exhibit 5). Furthermore, we find that, among non-financial corporates, digital footprint size is associated with KEV exposure more strongly than their annual revenue.

Exhibit 5

Exposure rises with digital footprint* and revenue size

Average monthly share of issuers with KEVs observed for at least 45 days during 2025, by digital footprint and revenue percentile rank



*Digital footprint is measured based on the number of Internet-facing assets. Assets are externally accessible machines or services, which form part of the organization's public-facing infrastructure, reflecting active observed systems such as IP addresses, domains, hostnames, and mobile applications.
Sources: Moody's Ratings, Bitsight Technologies

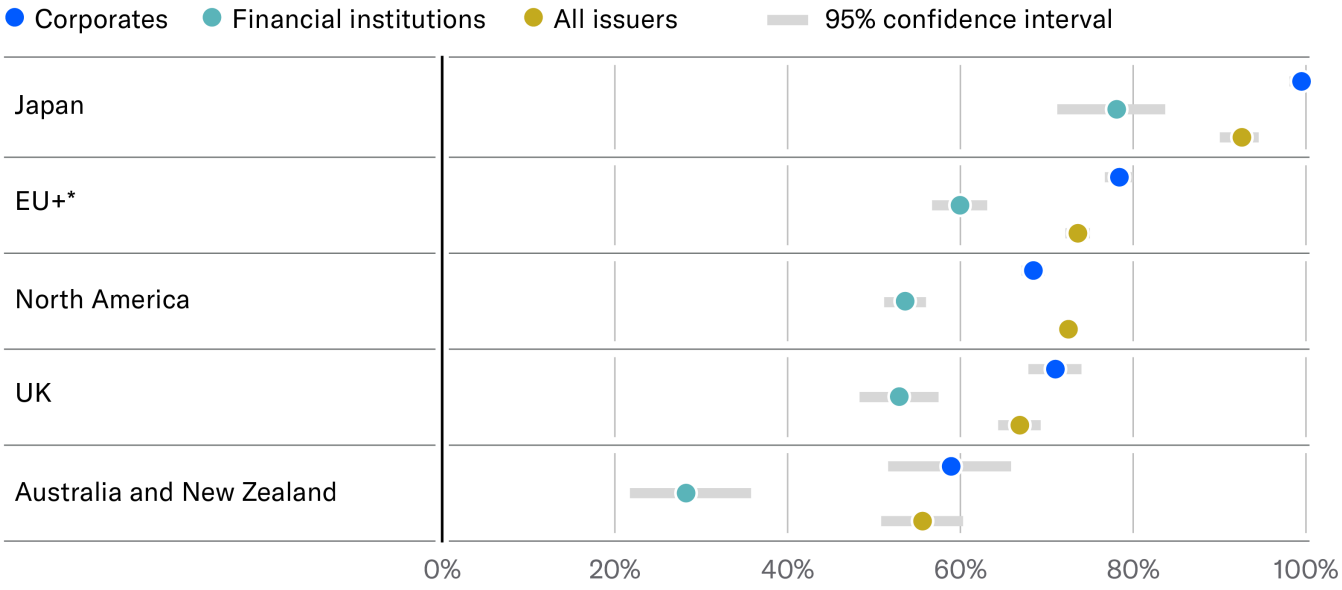
The strong relationship between KEV exposure and Internet-facing digital footprint is consistent with our earlier finding that larger entities experience disproportionately more cybersecurity incidents. It is also consistent with a finding by with Palo Alto Networks' Unit 42 that, in the largest enterprises, software vulnerabilities accounted for a greater share of illegal access than phishing. This is likely due to the complexity of large, sprawling operations with multiple ownership, legacy IT systems and uneven patching cycles. Together, these findings suggest that the underlying driver is not so much the size of a firm, but the scale and complexity of the externally exposed attack surface that often accompanies it.

Sector and regional factors remain material even after accounting for footprint size. We found that, even among issuers with comparably large Internet-facing footprints, e.g., those in the top 20% by digital footprint size, KEV prevalence varies markedly by region. Issuers in Japan still exhibit higher exposure, while issuers in Australia show the lowest exposure, relative to peers in North America, the UK, and EU+ (Exhibit 6).

Exhibit 6

Exposure to unresolved software weaknesses differs across regions

Average monthly share of large digital footprint issuers (top 20%) with KEVs observed for at least 45 days during 2025, by region and issuer type



*EU+ includes issuers in advanced economies in the EU, Iceland, Liechtenstein, Norway, and Switzerland.
Sources: Moody's Ratings, Bitsight Technologies

Patching outcomes vary

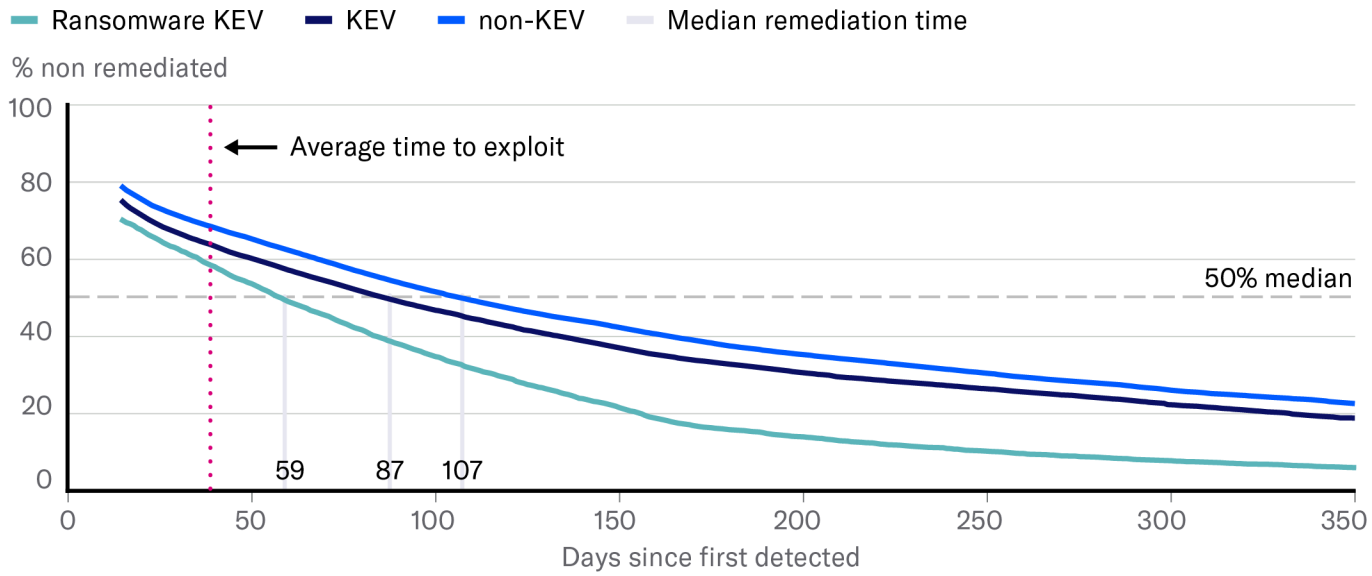
Our analysis of software bugs first detected over the last two years shows that organizations remediate known exploited vulnerabilities faster than other externally observed software flaws[5]. Ransomware-associated bugs are addressed fastest of all. This pattern holds across the full sample and within each sector, suggesting that issuers rightfully prioritize vulnerabilities with clear evidence of active exploitation.

It takes a typical issuer 107 days for half of non-KEVs to become no longer externally observable, according to our analysis. This compares with **87 days for KEVs** and 59 days for ransomware-associated KEVs (Exhibit 7). Even so, these median remediation times are slow when viewed against exploitation timelines. For example, security firm Flashpoint reports that the average time from public disclosure to first observed exploitation fell to 44 days in 2025 from 115 in 2024, highlighting how quickly exploitable software weaknesses can be weaponized once disclosed[6].

Exhibit 7

Remediation times lag the average time to exploit

Share of vulnerabilities that remain externally observable, by days since first detection* and vulnerability type



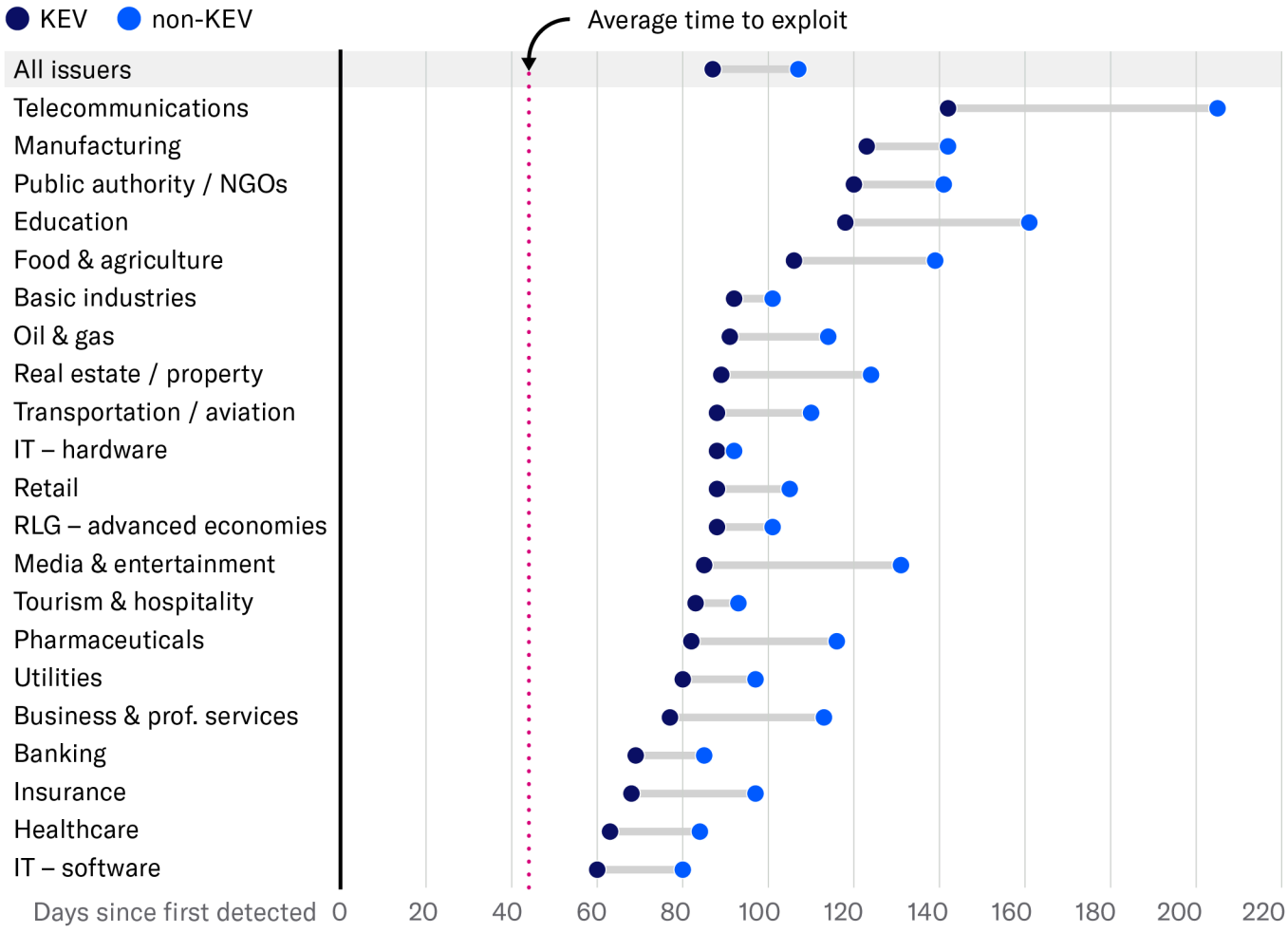
*We analyzed all vulnerabilities first observed in the last two years.
Sources: Moody's Ratings, Bitsight Technologies

Remediation performance varies significantly across sectors (Exhibit 8), and high exposure to unresolved KEVs does not always coincide with slow remediation. Some sectors, such as **education** and **telecommunications**, combine a high prevalence of +45 day KEVs with slower-than-average time to remediation. **Banking** performs well on both. By contrast, **IT software** companies combine high prevalence of KEVs with one of the shortest median remediation times, suggesting that high exposure can coexist with strong remediation capacity. Unlike KEV prevalence, however, remediation speed does not appear to show a clear relationship with the size of an issuer's external-facing digital footprint, with organizations with larger digital footprints and revenue performing on-par or better than those with smaller footprints.

Exhibit 8

Median time to remediate KEVs varies by sector

Time to remediate half of vulnerabilities by sector and vulnerability type



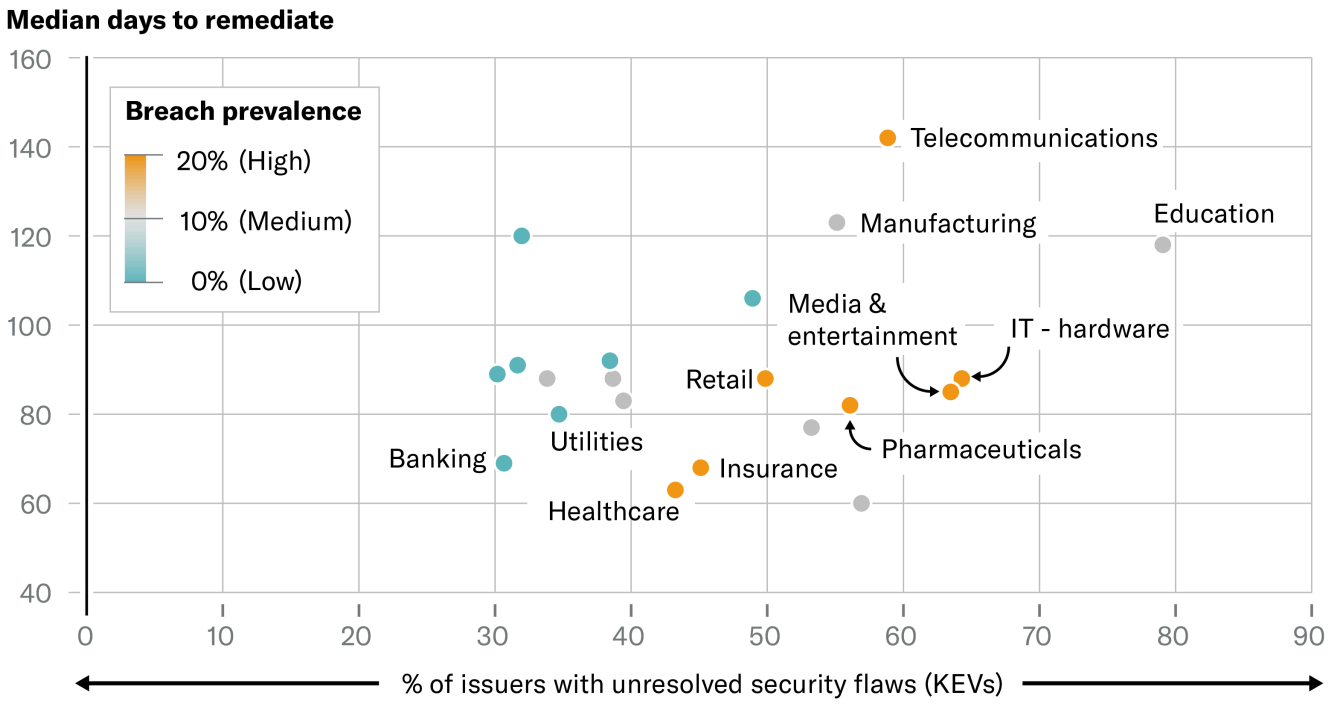
Sources: Moody's Ratings, Bitsight Technologies

KEV prevalence correlates with a higher rate of cyber incidents

Within our sample of issuers, our analysis shows that KEV prevalence correlates with breach prevalence[7] (Exhibit 9). Higher-exposure sectors exhibit, on average, higher rates of cyber incidents. The same applies at the regional level, with issuers in Japan and Korea having experienced the highest prevalence of cyber incidents in the past two years.

By contrast, there is no clear relationship between average remediation speed and breach prevalence. Measures like the "median days to remediate" describe how a typical organization performs, but breaches are more often driven by the few serious vulnerabilities that remain unaddressed for a long time. Because attackers only need one viable weakness, even a small number of long-standing, high risk issues can significantly increase exposure.

Exhibit 9
Sectors with higher prevalence of unresolved KEVs* show higher breach prevalence**



*Share of issuers in each sector with a KEV that remained unpatched for 45 days or more in February 2024; ** Share of issuers in each sector with at least one cyber incident in the subsequent two years.
Sources: Moody's Ratings, Bitsight Technologies

Endnotes

1 Internet-facing footprint refers to externally accessible systems and services - such as public websites, login pages, remote access tools, and online applications - that together make up an organization's visible digital attack surface.

2 The 9,500 issuers analyzed in this report include most rated corporates, financial institutions and a large subset of public infrastructure and public finance issuers.

3 These counts reflect observed vulnerability instances - defined by a specific vulnerability appearing on a specific asset over a given period, rather than a simple count of distinct vulnerability IDs. As a result, the same vulnerability may be counted multiple times if it affects multiple systems.

4 We measure digital footprint based on the number of an organization's Internet-facing assets. Assets are externally accessible machines or services that form part of an organization's public-facing infrastructure, reflecting observed, active systems such as IP addresses, domains, hostnames, and mobile applications. Asset importance is assessed by Bitsight using observable interaction patterns—including web traffic and the nature of the service provided—with the highest scoring assets classified as "critical". The asset counts used in this report include only critical assets directly controlled by the organization, and exclude assets operated on behalf of customers.

5 Since our analysis is based on external scanning rather than internal vulnerability scans, we measure the time from first detection until a vulnerability is no longer externally observable, rather than the precise internal remediation timelines. A vulnerability is treated as closed if it is no longer observed for 15 days after its last observed date, and as open if it is still observed within 60 days of the latest scans, unless more recent explicit remediation evidence is available.

6 This comparison is very conservative, as new vulnerabilities typically take days or even weeks to be researched and detected by Bitsight. As a result, this comparison likely understates the true speed advantage of attackers.

7 Breach prevalence is estimated based on Bitsight's breach data restricted to cybersecurity incidents affecting our sample of issuers. These incidents include a wide range of cyberattacks where unauthorized access has led to a confirmed data breach or business disruption.

within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.

REPORT NUMBER 1472151

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454