

# Cyber Conflict and the Erosion of Trust Introducing the Cyber Resilience Scorecard

**Safeguarding Trust, Economy, and Society**

SecurityScorecard  
World Economic Forum  
Annual Meeting 2024, Davos

# Executive Summary

Cyber threats reach beyond physical and economic disruptions to undermine societal trust, particularly in governments and the economy.

Why does this matter on a global scale? Trust drives revenue in the private sector and engagement in the public sector. Trust isn't abstract – you can earn and strengthen it.

## **Cybersecurity resilience is inextricably linked to trust**

Organizations' ability to thwart and rebound from cyberattacks directly influences confidence in the economy. While global leaders understand the importance of trust in our digital ecosystem, there is a lack of clarity on how to measure cybersecurity resilience.

Against this backdrop, our report explores the intricate dynamics between cyber threats, economic resilience, and the vital component of societal trust.

**“Ransomware is a threat to national security, public safety, and economic prosperity.”**

US National Cybersecurity Strategy for 2023

## CYBER RESILIENCE SCORECARD 2024

SecurityScorecard introduces the Cyber Resilience Scorecard, offering leaders and decision-makers a comprehensive view of global cyber risk.

Our study evaluates geographic regions worldwide for cyber risk preparedness and assesses its correlation with GDP — not only in their own organizations but also in that of their partners and vendors. We also present insights into threat actors' identities and the geographical origins behind cyber incidents.



# Key Findings:

## 1 Cyber risk vs. GDP

Exposure to cyber risk **strongly correlates** with a region's GDP.

## 2 Ten threat actor groups are responsible

for **44%** of global cyber incidents.

## 3 Geopolitical hotspots

Certain threat actors are concentrated in specific countries; notably, **24%** of cyberattacks originated from China, and the Russian Federation accounted for **15%**.

## 4 Risk interdependencies among industries

There is a **complex matrix of risk** interdependencies among different industries, necessitating comprehensive risk management strategies.

## 5 Critical sectors at risk

The **information services and technology** industries are most affected, followed by critical infrastructure sectors, such as: telecommunications, financial services, and government.

## 6 Interconnected supply chain risk

As cited by the new SEC cybersecurity incident disclosure requirements, SecurityScorecard research found that **98% of organizations use a third party that has been breached.**

These findings provide critical insights for policy-makers, business executives, and cybersecurity professionals in understanding and addressing the evolving landscape of cyber threats and resilience.

Anne Neuberger, U.S. Deputy National Security Advisor for Cyber and Emerging Technology, observed:

**“It is always wise for countries to have good visibility. The first step in an effective cybersecurity practice is having good visibility of one's networks.”**

# Methodology

SecurityScorecard maintains and continuously updates cybersecurity ratings on more than 12 million entities worldwide. We monitor over 250+ different types of signals pertaining to various aspects of cybersecurity, including: network security; endpoint security; patching cadence; and others.

SecurityScorecard has developed a data-driven cybersecurity scoring system using artificial intelligence, proprietary threat intelligence, and publicly available reports of data breaches to assess, continuously monitor, and quantify an organization's cyber risk.

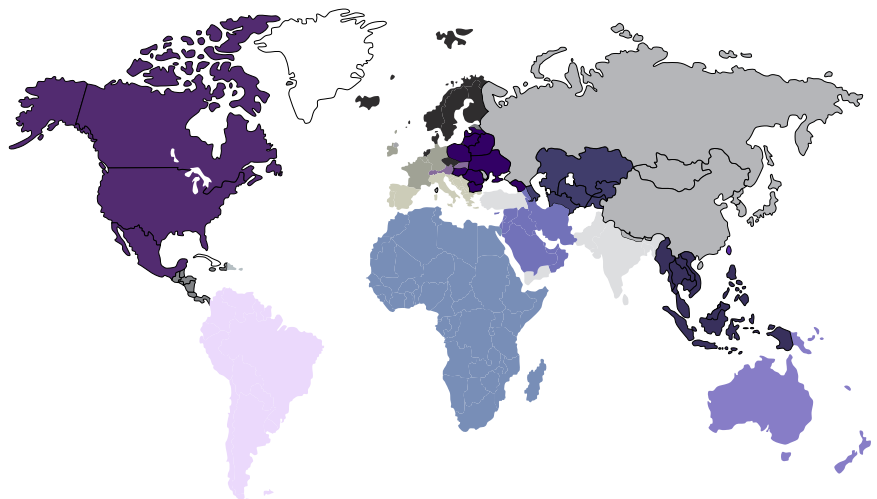
To develop the Cyber Resilience Scorecard, threat intelligence analysts analyzed the cybersecurity hygiene scores across 6.3 million entities situated in 189 countries located in 17 geographic regions around the world and combined this data with [2022 GDP per capita economic data](#) published by the IMF.

The 6.3 million organizations represent a random selection of nearly half of the entities for which we have data in the United States and all organizations for which we have data globally. Regional cybersecurity hygiene scores and GDP per capita were calculated using the means of the associated country hygiene scores and GDP per capita data. Our division of the globe into 17 geographic regions is depicted in Figure 1.

**Threat intelligence analysts analyzed the cybersecurity hygiene scores across 6.3 million entities situated in 189 countries located in 17 geographic regions around the world.**

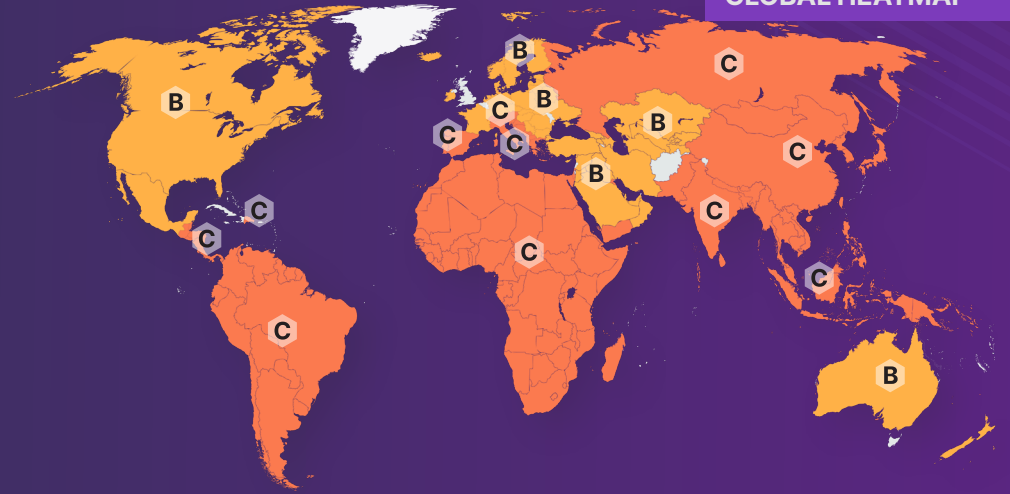
**FIGURE 1:**  
**Cyber Hygiene around the world**

- Africa
- Caribbean
- Central America
- Central Asia and the Caucasus
- Central Europe
- East Asia
- Eastern Europe
- Middle East
- North America
- North East Asia
- Northern Europe
- Pacific
- South America
- South Asia
- South East Asia
- Southern Europe
- Western Europe



# Results

## GLOBAL HEATMAP



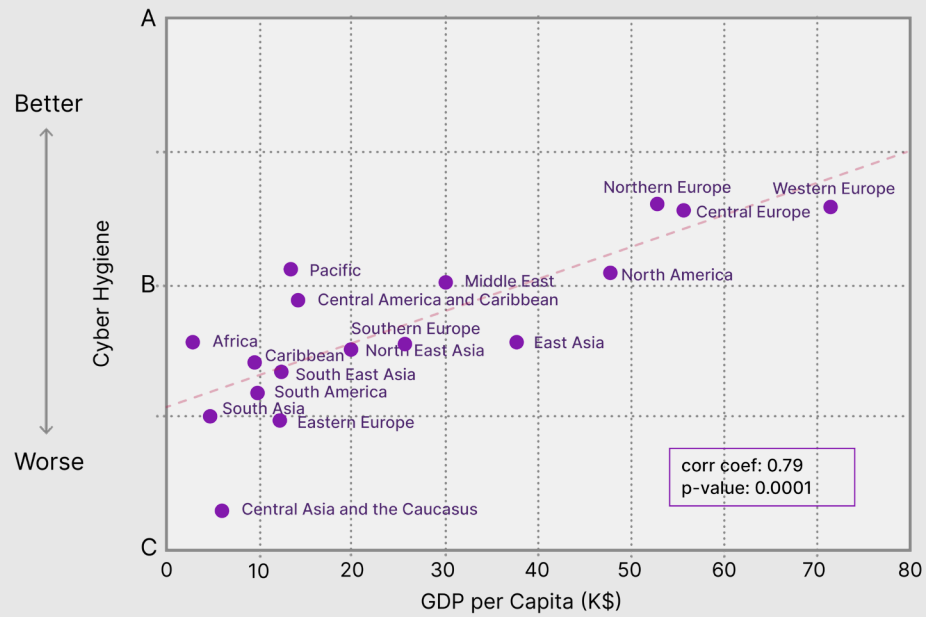
**FIGURE 2:**  
**The Cyber Resilience Scorecard**

Region	Security Score	Cyber hygiene	2022 GDP per capita	Countries	Entities
Northern Europe	B	82.97	\$52,940.24	9	950,303
Western Europe	B	82.85	\$71,381.04	6	580,681
Central Europe	B	82.78	\$55,704.08	3	455,927
Pacific	B	80.48	\$13,379.22	13	337,088
North America	B	80.37	\$47,548.44	3	709,138
Middle East	B	80.07	\$30,116.12	12	106,487
Central America and the Caribbean	C	79.31	\$6,170.23	7	23,248
East Asia	C	77.78	\$37,558.06	4	121,165
Africa	C	77.77	\$2,861.27	52	179,726
Southern Europe	C	77.66	\$25,651.17	12	666,604
North East Asia	C	77.45	\$19,908.02	5	461,181
Caribbean	C	76.96	\$9,586.72	2	1,203
South East Asia	C	76.65	\$12,361.00	10	267,919
South America	C	75.83	\$9,602.92	12	433,251
South Asia	C	74.93	\$4,694.69	9	267,928
Eastern Europe	C	74.73	\$12,244.47	11	769,462
Central Asia & the Caucasus	C	71.73	\$6,170.23	7	23,248

A summary of the data is presented in the Cyber Resilience Scorecard (Figure 2), with tallies of the number of countries and the number of organizations contributing to the grade for each region. Overall, the scores range from a low C (Central Asia and the Caucasus) to a low B (Western Europe). No region scores above a low B, with most regions falling in the C range. Notable outliers include the Pacific region, which has a higher score than its GDP per capita would predict, and Central Asia and the Caucasus, which has a lower score than its GDP per capita would predict.

As shown in the scatter plot of scores and GDP per capita (Figure 3), there is a statistically significant ( $p$ -value < 0.0001) positive correlation between a region's cybersecurity hygiene and its per capita GDP (correlation coefficient = 0.79).

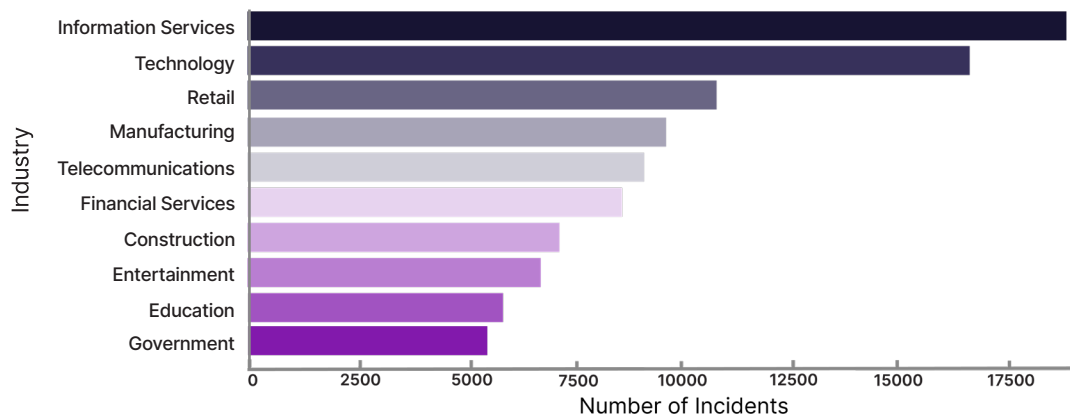
**FIGURE 3:**  
**Cyber hygiene vs. GDP per Capita**



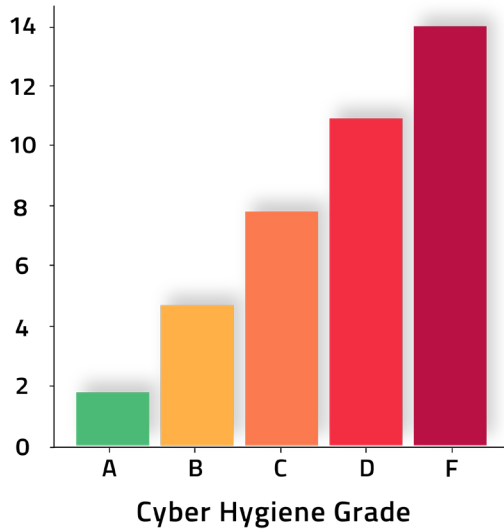
Regions with higher per capita GDP tend to exhibit better cybersecurity hygiene and lower cyber risk. Presumably, wealthier economies are better equipped to invest in resilient and safe infrastructure and to implement and maintain active security programs to combat the ever-evolving nature of cyber threats. Wealthier countries may also be more likely to use licensed software that is kept up to date with security patches.

SecurityScorecard identified over 110,000 security incidents in our data holdings. Organizations in the information services and technology industries, including major tech companies and consulting firms, are the most affected by breaches, according to our data (Figure 5). Critical infrastructure is also represented on the list: telecommunications, financial services, and government. Note in particular the interdependencies among these industries, and indeed economies more broadly – all rely to varying degrees on information services, technology, and telecommunications.

**FIGURE 4:**  
**Top ten industries affected by breaches**



**FIGURE 5:**  
**Breach likelihood ratio**



**As we have previously observed:** The result of these interactions is a complex matrix of risk interdependencies that policy-makers and business executives around the world are attempting to address with laws, policies, and risk management strategies. A key missing ingredient in many of these initiatives is an emphasis on the measurement of risk outcomes.








Using this data, we are able to calculate the likelihood that an organization with a given grade will suffer a breach, in comparison to organizations with a baseline grade of A (Figure 6). For regions whose organizations have an average score of B, organizations in that region are nearly three times as likely to suffer a cyber breach compared to the baseline A grade. Regions whose organizations have an average score of C are nearly five-and-a-half times as likely to suffer a cyber breach, or nearly double the probability associated with a grade of B.

**FIGURE 6:**  
**Breach likelihood**

Grade	Breach Likelihood
<b>A</b>	1x
<b>B</b>	2.9x
<b>C</b>	5.4x
<b>D</b>	9.2x
<b>F</b>	13.8x

## 7 factors most predictive of a breach

By analyzing Security Ratings and cyber insurance claims data, research with the Marsh McLennan Global Cyber Risk Analytics Center Identified seven factors most predictive of a breach:

-  ENDPOINT SECURITY
-  PATCHING CADENCE
-  RANSOMWARE SCORE
-  NETWORK SECURITY
-  DNS HEALTH
-  IP REPUTATION
-  CUBIT SCORE

**The average global cost of a data breach is \$4.5M.**

IBM Security,  
Cost of Data Breach Report 2023

# Who's Behind Malicious Activity?



In many cases, we can also discern the identity of the threat actor behind incidents, including the geographic region from which they operate. Ten threat actor groups account for 44% of the incidents in our data holdings:

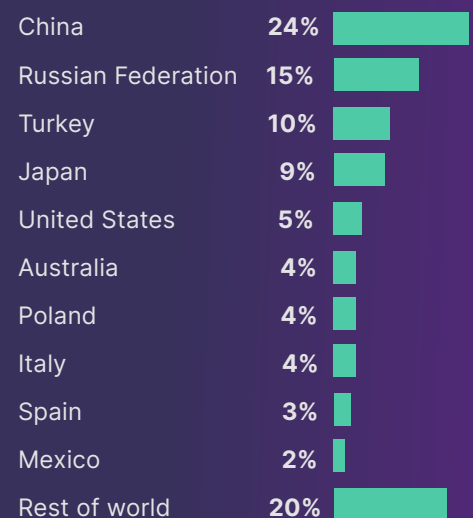
- 1 APT28:** This group is responsible for over 6.32% of the incidents, making it the most active threat actor in the dataset.
- 2 Cobalt Group:** Accounts for 5.80% of the incidents.
- 3 Sandworm Team:** Represents 5.02% of the incidents.
- 4 Equation Group:** Contributes 4.89% to the total number of incidents.
- 5 APT41:** Responsible for 4.85% of the incidents.
- 6 Earth Berberoka:** Accounts for 4.38% of the total incidents.
- 7 APT40:** Contributes to 3.48% of the incidents.
- 8 Energetic Bear:** Also contributes to 3.48% of the incidents, closely matching APT40.
- 9 Leafminer:** Makes up 2.91% of the incidents.
- 10 Luckycat APT:** Accounts for 2.88% of the incidents.

These and other threat groups operate globally, but their operational infrastructure is concentrated in some countries more than others. The fact that a threat actor operates from a particular geography does not necessarily mean that the threat actor is physically located there: threat actors often develop their operational infrastructure in multiple countries or regions to obscure their identity and enhance the resilience of that infrastructure against defensive efforts to disrupt it. It does mean, however, that the geography in question is host to operational infrastructure, which is often in the form of compromised information systems owned or operated by unwitting third parties.

According to our data (Figure 7), nearly one-quarter of incidents originate from China, making it the leading source of cyber incidents. The Russian Federation is next, accounting for 15% of incidents. The United States accounts for over 5% of incidents. Given the breadth of per capita GDP among the countries in Figure 7, there does not appear to be a strong correlation between per capita GDP and serving as the origin for malicious cyber activity.

FIGURE 7:

## Cyber incident origin by geographic location





According to 2023 Gartner Research, “transparency delivers 53% improvement in third-party cyber risk management effectiveness.”<sup>1</sup>

# Implications and Recommendations

As Jen Easterly, the head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), testified to the U.S. Congress in 2021, “I think it’s hard to say you’ve reduced risk unless you know how to measure it.” SecurityScorecard wholeheartedly agrees: data makes it possible to turn knowledge of cyber risk exposure into action.

Our analysis of regional cybersecurity resilience is built on data about specific organizations’ cybersecurity risk posture. Using this data, business leaders can derive actionable insights not only about the cybersecurity risk posture of their own organizations, but their business partners too, in order to manage third-party risk.

These insights about individual organizations, in turn, can be further aggregated to illuminate the cyber risk posture of entire sectors, such as: energy, water, or other critical infrastructure – giving national leaders and regulators data-driven insights into the performance of key sectors of national importance. Such data can be used to inform regulatory policy and facilitate public-private partnerships by establishing a shared understanding of risks, vulnerabilities, and the steps needed to address them.

In this context, cyber risk ratings emerge as a potent tool for creating needed transparency. Just as credit ratings provide a clear and standardized measure of financial credibility, cyber risk ratings can offer a similar benchmark for cybersecurity posture.

The availability of objective data on cybersecurity resilience gives business and government leaders a new language for cyber risk management – one that permits them to be relentlessly data-driven about managing cybersecurity risk. To paraphrase the old Russian proverb “trust, but verify,” data on cybersecurity risks helps build trust by enabling business and national leaders to verify the cybersecurity posture of organizations, business partners, and even critical infrastructure.

As the Forum convenes this week under the theme of Rebuilding Trust, we believe this analysis provides a roadmap to assess and communicate progress in reducing cyber vulnerabilities continuously to enhance resilience and trust among global stakeholders.

## A Roadmap to Cyber Resilience: 6 Essential Steps

- 1** Embrace cybersecurity transparency
- 2** Track key threat actors
- 3** Forge industry coalitions to address shared cyber risk
- 4** Establish clear cybersecurity metrics
- 5** Create a global cybersecurity scoring framework for all
- 6** Make cybersecurity a core business imperative

1. Gartner, Inc., CISO Edge Podcast: Wrangling Third-Party Cybersecurity Risk, Christopher Mixter, Rahul Balakrishnan, November 29, 2023.

To learn more and create  
your free account, visit  
[SecurityScorecard.com](https://SecurityScorecard.com)

## ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent [Instant SecurityScorecard rating](#). For more information, visit [securityscorecard.com](https://securityscorecard.com) or connect with us on [LinkedIn](#).



[SecurityScorecard.com](https://SecurityScorecard.com)  
[info@securityscorecard.io](mailto:info@securityscorecard.io)

United States: (800) 682-1707  
International: +1(646) 809-2166



©2024 SecurityScorecard Inc. All Rights Reserved.