MASTERCARD RISKRECON • RISK POSTURE ANALYSIS
CANADA • JULY 2025

Cyber risk in Canada

Industry trends and observations

Contents

Why cyber risk management matters

Cyber risk management is critical for Canadian organizations to protect their assets and maintain customer trust. With the rise of sophisticated cyber threats — such as ransomware, phishing, and data breaches — it is imperative that businesses adopt proactive security strategies to mitigate financial, operational, and reputational risks.

In this white paper, RiskRecon dives into key cyber insights and observations of over 4,900 Canada-based organizations based on the analysis of collected cyber hygiene data.* Many of the industries covered represent critical infrastructure and are integral to the safety and security of Canadian businesses. As such, this report focuses on the largest cyber risk areas across industries, demonstrating the growing importance of embedding cyber risk mitigation strategies within organizations to help counter risks when they arise.

By taking a proactive approach, Canadian businesses can strengthen their security posture, and foster a culture of cyber trust and innovation. RiskRecon and Mastercard are committed to helping businesses protect themselves from evolving cyber risks to ensure the safety and strength of the Canadian ecosystem.

*Survey conducted in 2024 through an analysis of Canadian based entities within RiskRecon.

The purpose of this report is to provide insight into broader cyber practices of private, public, and government organizations across 14 industries in Canada, covering:

- Agriculture/forestry/fishing/hunting
- Arts and entertainment
- Construction/warehousing
- Education
- Finance/insurance
- Healthcare
- Information/computers/software
- Manufacturing
- Oil and gas
- Retail trade
- Science/technical
- Transportation
- Utilities
- Wholesale trade

RiskRecon has passively evaluated the security and infrastructure safeguards and gaps for Canadian organizations on over 40 criteria across nine security domains including:

- Email security
- Breach events
- Network filtering
- DNS security
- System reputation
- Web encryption
- Application security
- Software patching
- System hosting

This information was then assessed for impact of each vulnerability uncovered to determine an organization's final cyber risk rating.

Cyber risk observations across industries in Canada

The following section provides an analysis of cyber hygiene and performance trends by industry across 4,900 organizations within Risk Recon. For each organization assessed, RiskRecon generates a cyber risk rating that is derived from a combination of asset value and issue severity. These results have been aggregated across Canada and by industry to provide insightful cyber risk observations.

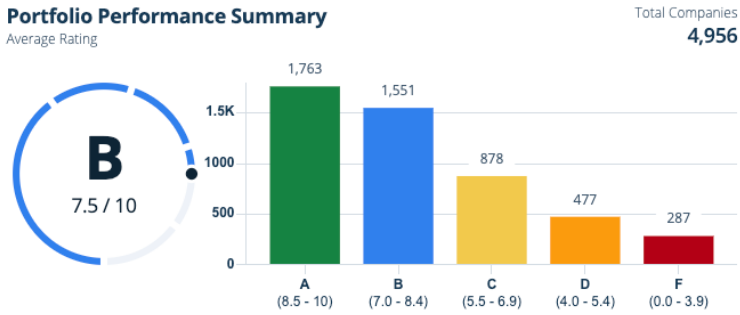
Observation 1:

Canadian organizations have good cyber hygiene despite being considered adopters in the cybersecurity space

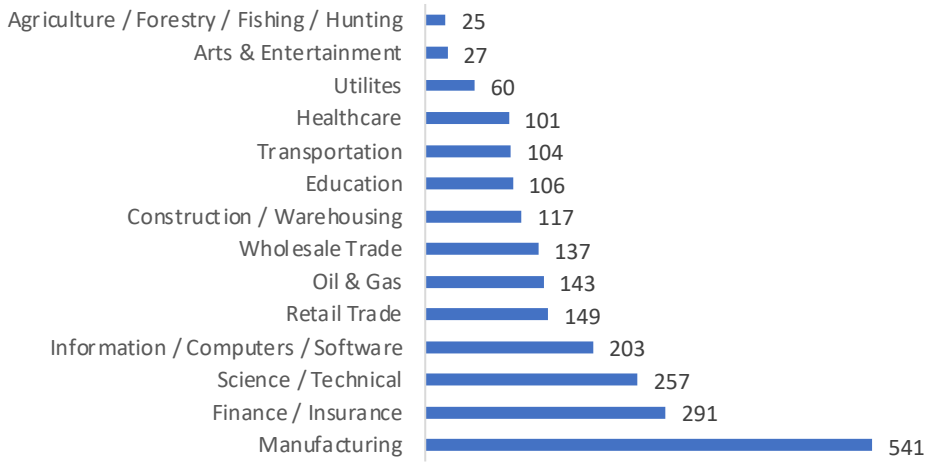
RiskRecon rates the quality of an organization's cybersecurity risk performance using an A–F labeled scale and 0-10 numeric scale. The rating is based on the ratings and risk priority of issues present in the environment as observed by RiskRecon's passive risk assessment technology. Canada-based organizations surveyed have an average cybersecurity rating (B/7.5), with 36% of those organizations securing a high rating (A/8.5-10). Generally, 66% of all organizations fall within an average to high rating (A/B), indicating that Canadian companies have good cyber hygiene reflective of their public assets.

The remaining 33% of Canadian organizations are decreasingly distributed on a C-F rating scale, which is indicative of higher-priority cyber risk issues. It is important to note that some of this performance may be influenced by a high concentration of small to medium sized organizations that typically perform at extreme ends of the rating scale.

Figure 1: Distribution of RiskRecon cyber ratings across 4,956 Canadian organizations on an A-F (0-10) scale



RiskRecon distribution of organizations in Canada by industry



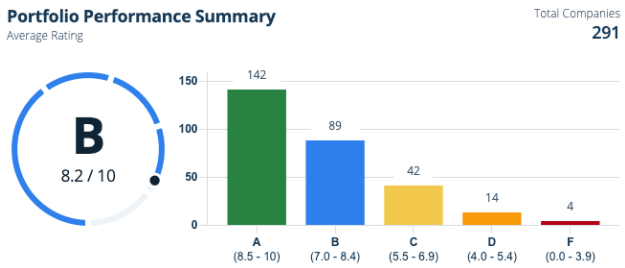
Observation 2:
Cyber hygiene is relatively stable by industry, with some nuances driven by industry specific factors

The table below provides a score and rating breakdown across various industries. Many industries demonstrated positive performance on average with insurance and financial, retail trade, and utilities showing as the top performing industries from a cyber hygiene standpoint. Some industries showed considerable variability in rating distribution, suggesting that the industry may face trending cyber-related issues that are driving the score down. These issues are explained further in the report.

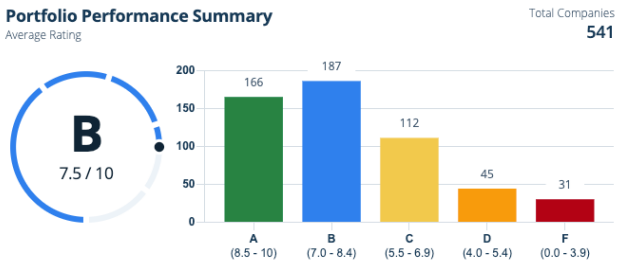
While all industries comprise of organizations that perform quite well, some industries have a higher volume of low performing organizations or organizations that currently hold high-risk issues. These high-risk issues are prioritized based on the severity of the issue as well as the aggregate impact of the issue.

Figure 2: Distribution of RiskRecon cyber ratings by industry on an A-F (0-10) scale

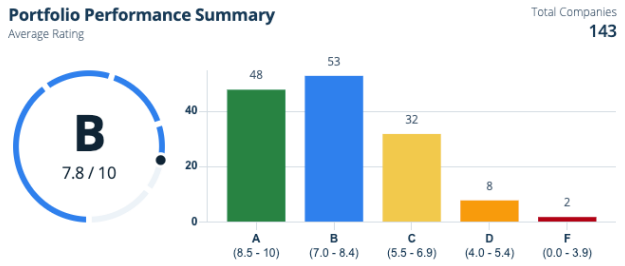
Insurance and financial



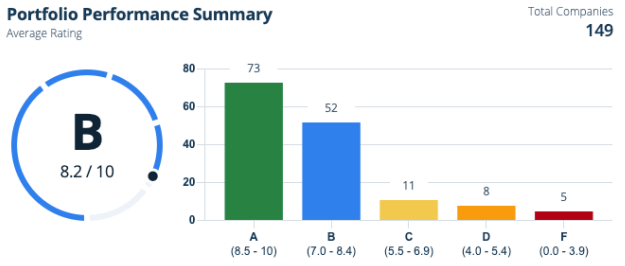
Manufacturing



Oil and gas

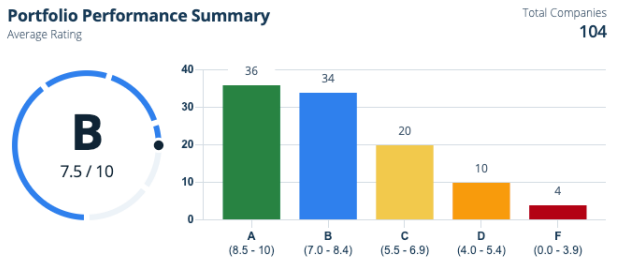


Retail trade

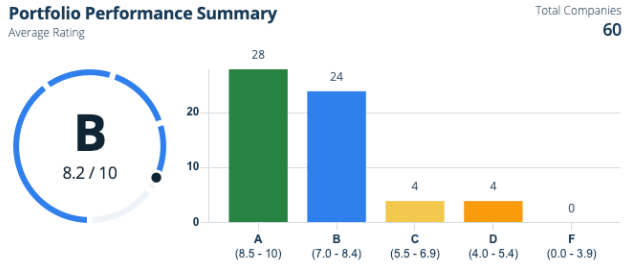


Scientific and technical

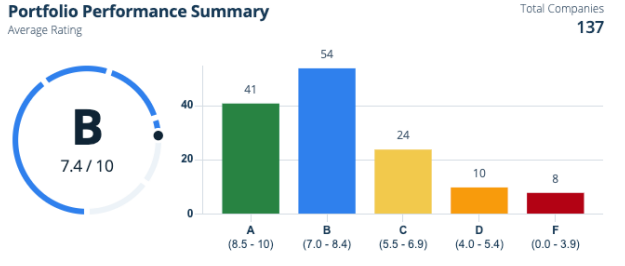
Transportation



Utilities



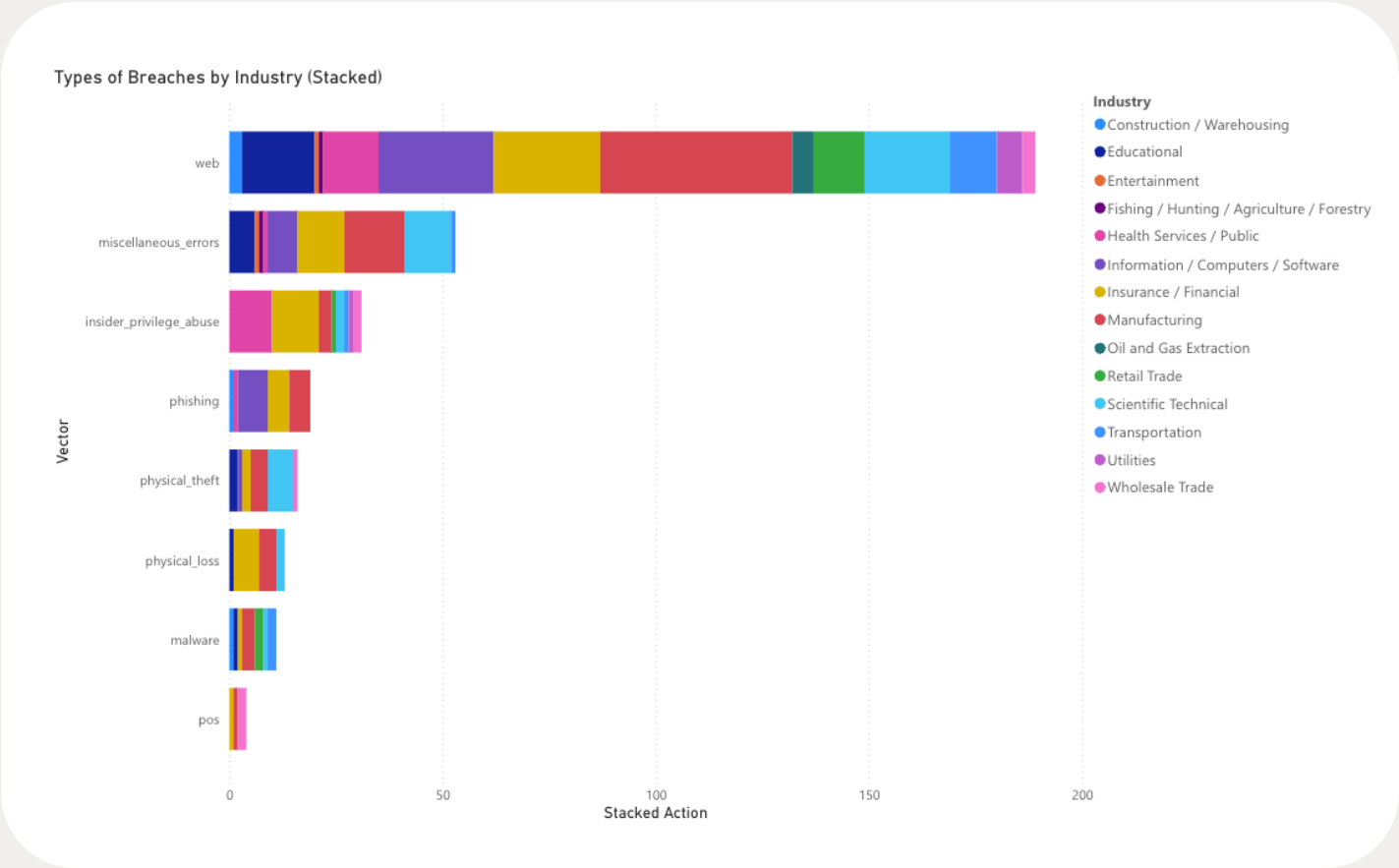
Wholesale trade



Observation 3:
All industries in Canada are struggling with a massive prevalence of web attacks

As demonstrated below, all industries are facing a high volume of web attacks in comparison to other types of breaches like insider privilege abuse, phishing, and physical theft. Web attacks have been included after a thorough vetting process across seven external sources by the RiskRecon platform.

Figure 3: Types of breaches across industries in Canada



Observation 4:
Some industries like manufacturing, information security, and education are facing a higher volume of medium to high-risk cyber issues

To drill down into what may be driving a lower cyber rating for an industry, we broke down the issues by severity across industry. The severity of an issue in RiskRecon is heavily influenced by several types of inputs which contribute to the cyber rating:

- Software patching concerns
- Exposed services (open ports)
- Publicly accessible IoT devices
- Unencrypted sensitive systems

Following the methodology outlined in this section, RiskRecon has provided a breakdown of organizations by industry to provide additional insight into areas of specific concern that may be of interest to the appropriate responsible parties within Canada. The following section provides a view of cyber hygiene and performance across all organizations identified in Canada.

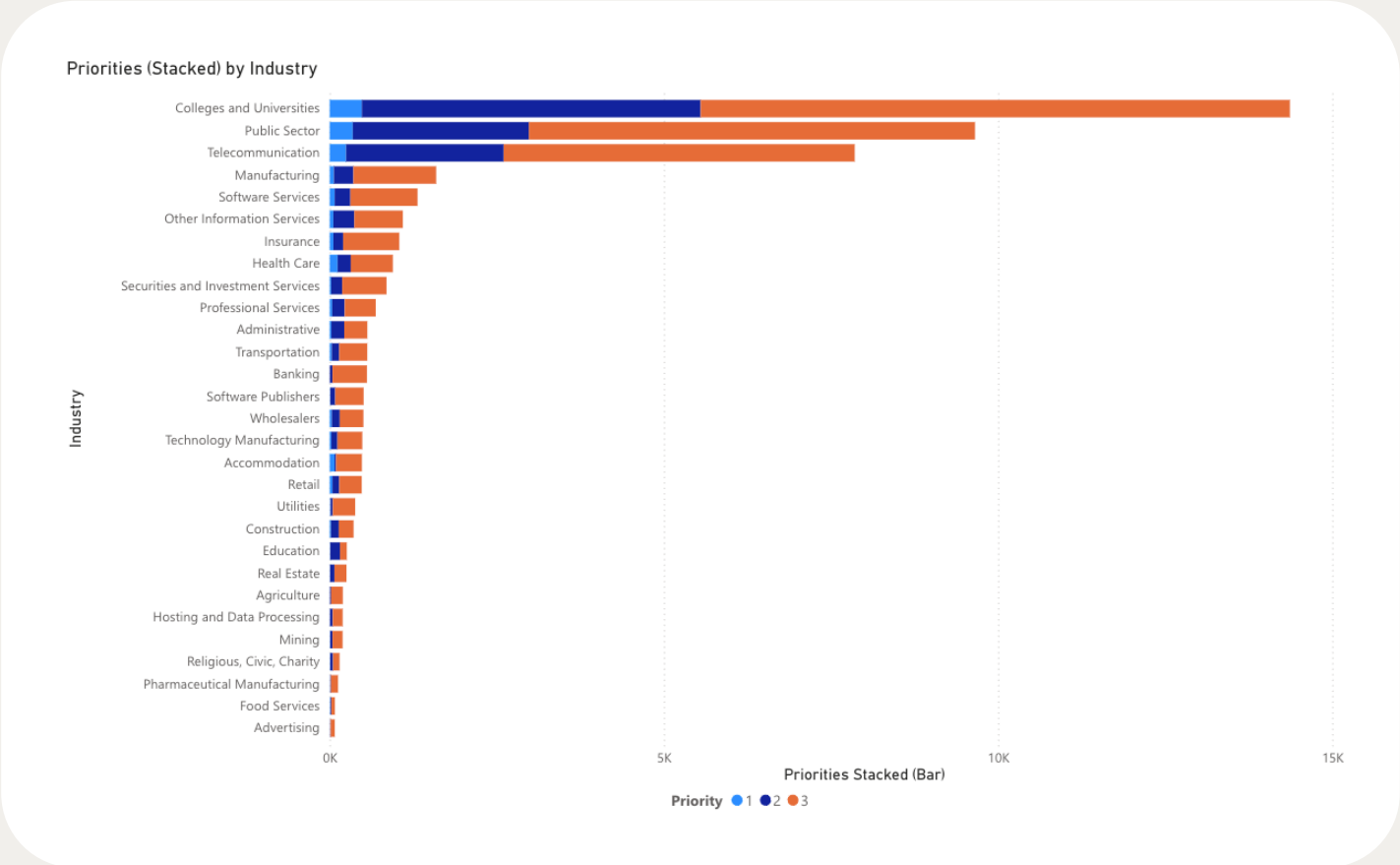
The below chart provides a summary of the concentration of high-risk issues across each industry, ranked by issue severity (Priority 1 is high, Priority 2 is medium and Priority 3 is low). While the overall portfolio rating average of B/7.5 is positive, several organizations show higher levels of Priority 1, Priority 2, and Priority 3, which are considered highest risk.

Analyzing the graph above, one can see that colleges and universities have the most Priority 1, 2, and 3 issues combined. This may be attributed to this industry's normal collective information sharing model.

Additionally, while both public sector and telecommunication face some Priority 1 issues, the cleanup of several Priority 3 issues could lend to a better score with some low-hanging concerns remediated.

Finally, manufacturing, information, and scientific and technical industries are facing the highest volume of issues, suggesting that there are gaps in the methods to address cybersecurity risks. An in-depth analysis of the driving factors behind issue volume is described below; for the purposes of this report, we have focused on high severity issues (Priority 1). It is also important to note that the volume of issues driving an industry may be a result of a higher number of companies present within that industry.

Figure 4: Number of issues by risk priority across industries in Canada



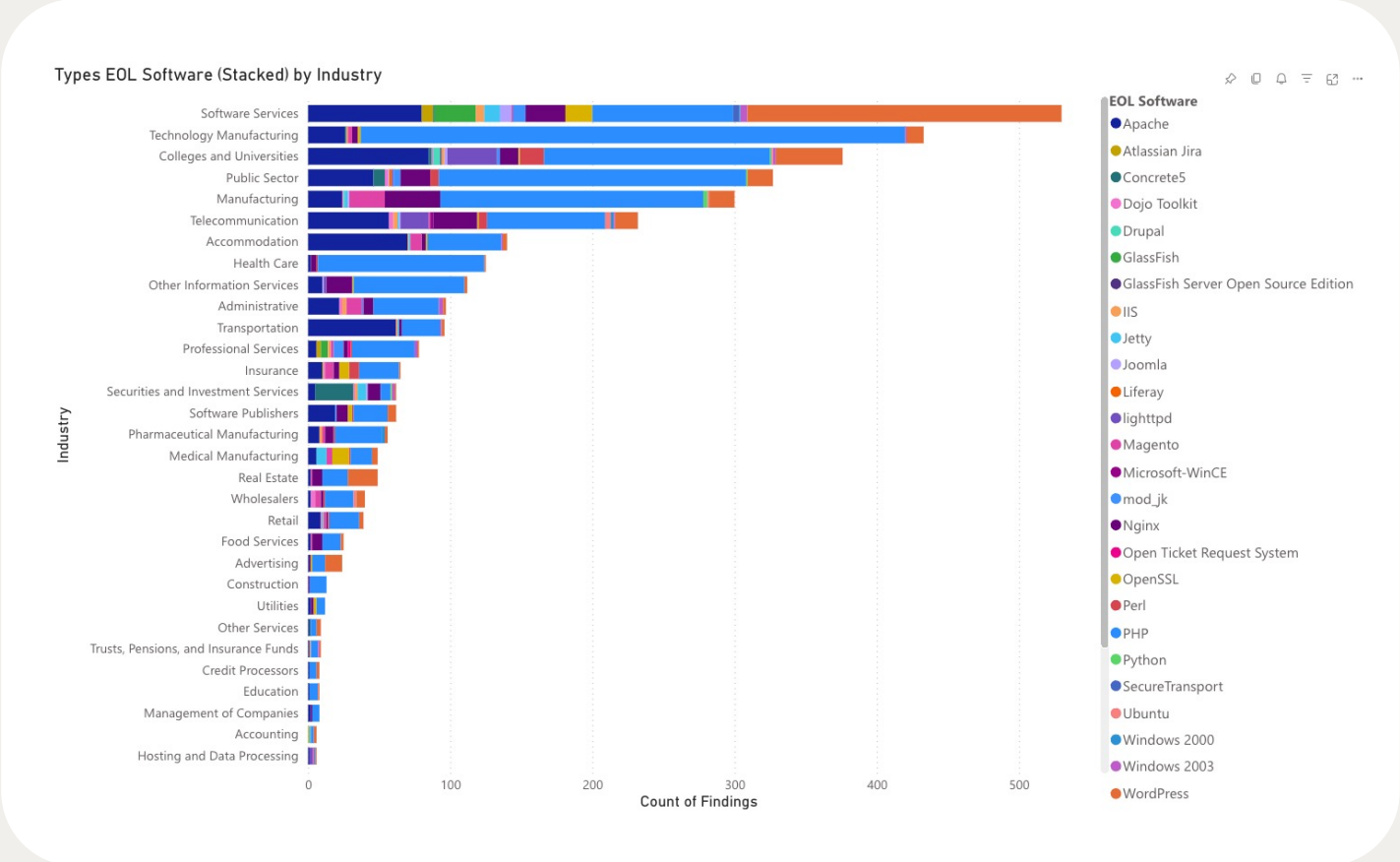
Observation 5:

The software services industry faces significant risks of data breaches due to the use of unsupported or end-of-life software

Software patching performance and, specifically, the presence of unsupported or end-of-life (EOL) software (meaning the manufacturer of the software no longer provides patches or protection against vulnerabilities, should they arise) is a significant indicator of potential for data breaches or ransomware attacks.

The chart below provides a summary of the type and concentration of EOL software observed across for in-scope companies. As seen below, software services are highly susceptible to breaches related to EOL software. The majority of EOL software versions detected are versions of PHP (an application server) and Apache (a web server) which are particularly susceptible to critical vulnerabilities.

Figure 5: End-of-life and unsupported software types across industries in Canada



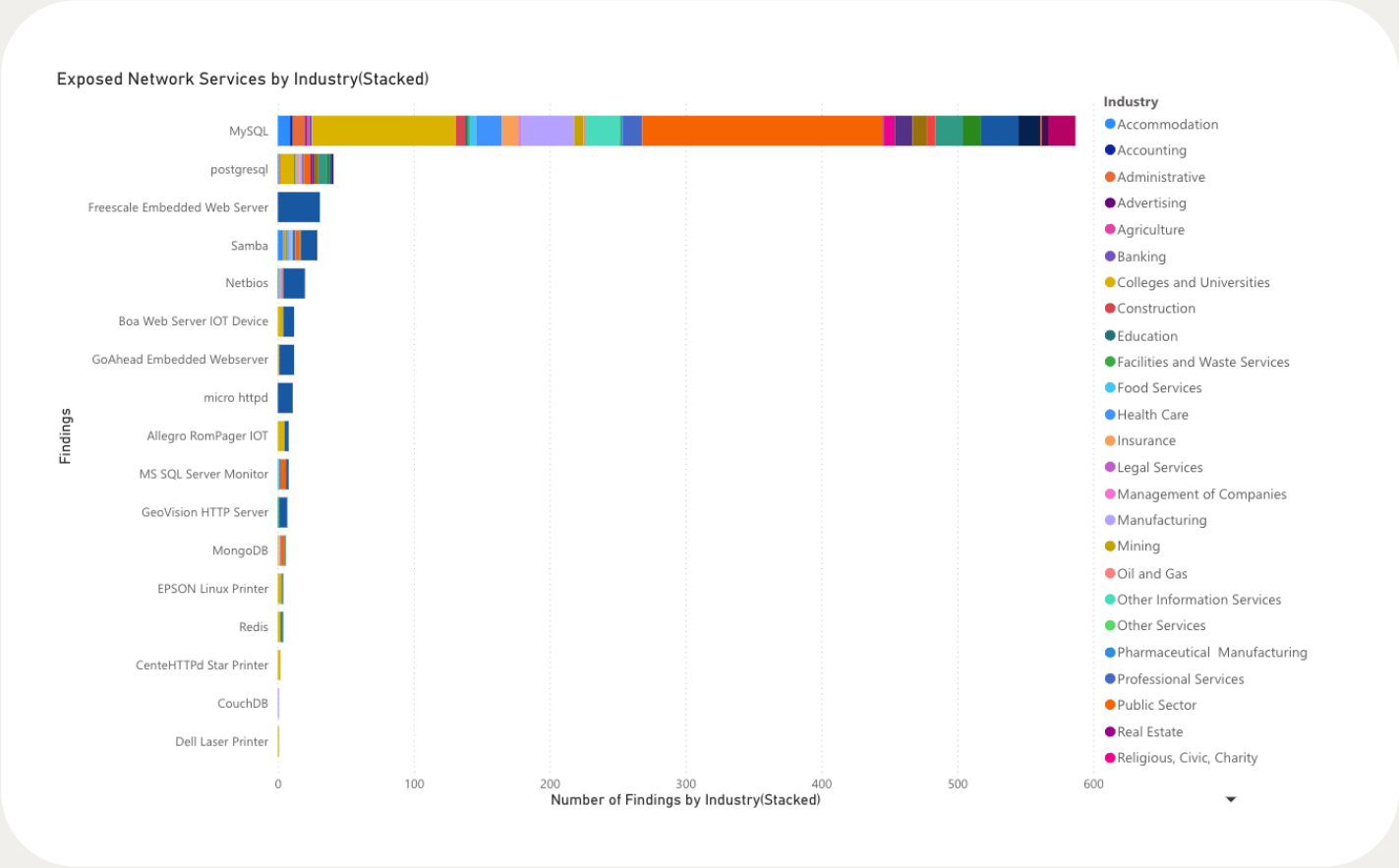
Observation 6:
The public sector, education and telecommunications industries face higher levels of exposed network services

RiskRecon's Network Filtering security domain provides information on organizations and their internet facing systems, including where appropriate filtering may not be in place. This is demonstrated by the presence of open/exposed ports (exposed services) or the presence of accessible "internet of things" (IoT) devices. These gaps represent potential entry points for malicious actors, and it is recommended that these entry points be appropriately filtered and protected.

RiskRecon uses a combination of direct observation and commercial data sources to identify systems where services or devices are exposed to the public internet. As seen below, the majority of concerns stem from MySQL server service which may expose non-public data or provide an attacker with control of the identified system. Clearly, the public sector, colleges and universities, and telecommunication industries have the most exposed network services, presenting a significant opportunity for malicious actors to enter systems.

It is important to note that the education sector may have industry specific justifications for a higher-than-normal volume of open ports and IoT devices. Particularly, most colleges and universities are part of a network infrastructure that lends itself to networks services being exposed either due to student activities or inter-collegiate data sharing.

Figure 6: Exposed network services by industry



Mastercard RiskRecon

RiskRecon is a cybersecurity risk management platform that provides automated, data-driven assessments of third-party cybersecurity risks. It enables organizations to evaluate and continuously monitor the security posture of third parties, partners, and other external organizations, helping businesses mitigate cyber threats in an increasingly interconnected landscape.

RiskRecon analyses provide cyber risk ratings for each organization monitored and further breaks down the overall rating into nine rated security domains which are further broken down into 36 discreetly rated sub-domains, referred to as security criteria which are supported by detailed findings, issue prioritization, and deep analytics capabilities.

RISKRECON DOES...

- Deep mining of domain registration databases
- Deep mining of network registration databases
- Analysis of Internet DNS IP to hostname resolution logs
- DNS queries
- Lightly browse web sites, obeying robots.txt instructions
- Analytics of publicly accessible code, content, configurations
- Monitoring and analysis of commercial and open-source IP reputation feeds
- Mining the internet for relevant information such as indicators of data loss events
- Analyze Internet port scan data sourced from a commercial provider

RISKRECON DOES NOT...

- Tamper with parameters
- Inject code
- Conduct cross-site scripting
- Conduct SQL injection
- Attempt to bypass authentication
- Execute memory overflow tests
- Fill out form fields
- Guess credentials
- Execute vulnerability exploits
- Attempt to bypass security controls

Key contacts

Interested in learning more?

Please reach out to Chetan Bhogal to explore how RiskRecon can add value to your organization.