WHITE PAPER

FEBRUARY 2022

The state of cybersecurity in U.S. cities

riskrecon

mastercard

Contents

Executive summary

It is widely recognized that cities and local government agencies within the United States have increasingly become targets of ransomware in recent years. In fact, on June 17, 2021, the United States Senate Subcommittee on Emerging Threats and Spending Oversight held a hearing on "Addressing Emerging Cybersecurity Threats to State and Local Government." The Committee Chair highlighted that the estimated cost of publicly known ransomware attacks impacting states and local governments in 2020 was approximately one billion dollars.

With COVID-19 accelerating the public's reliance on digital connectivity, more investment in technology and people is needed to improve the cyber resilience of local governments. Local governments are the providers of many critical services necessary for everyday life. Exploits of cyber vulnerabilities in the public sector can cause far-reaching impacts and interruptions to communities. Disruption of essential services is not the only risk posed by cybercriminals. Government organizations are unique because they hold vast amounts of sensitive and confidential data. Whether it be personally identifiable information on citizens, documents related to public safety and courts, or even communications on sensitive matters, the stolen data is often used in attempts for extortion and ultimately offered for sale to other criminals.

It is also known that as organizations continue to rely on third and fourth-party relationships for their critical business processes, over half of reported data breaches result from those relationships. Cities and local governments are no different. Now more than ever, cities are outsourcing and leveraging third parties for activities that range from website design and web hosting to parking ticket fine collection and utility payments.

As a result of the increased reliance on third parties, RiskRecon, a Mastercard Company, evaluated a sample of 271 of the most populated U.S. cities' government websites as of August 29, 2021, to assess their cybersecurity posture and subsequent third and fourth-party vendors that support our cities and local governments. [A full list of the U.S. cities included in the dataset can be found in **Appendix A**.]

Key Findings

59% **(161)** of cities fall into A and B ratings, indicating that their information security programs may be sufficient to protect their data assets

41% **(110)** of cities have C or below ratings, and two cities even have an F rating, indicating that there may be security gaps present in systems that could potentially result in data compromise

7.3/10 average cybersecurity rating for all city governments (corresponding to B rating).

In comparison

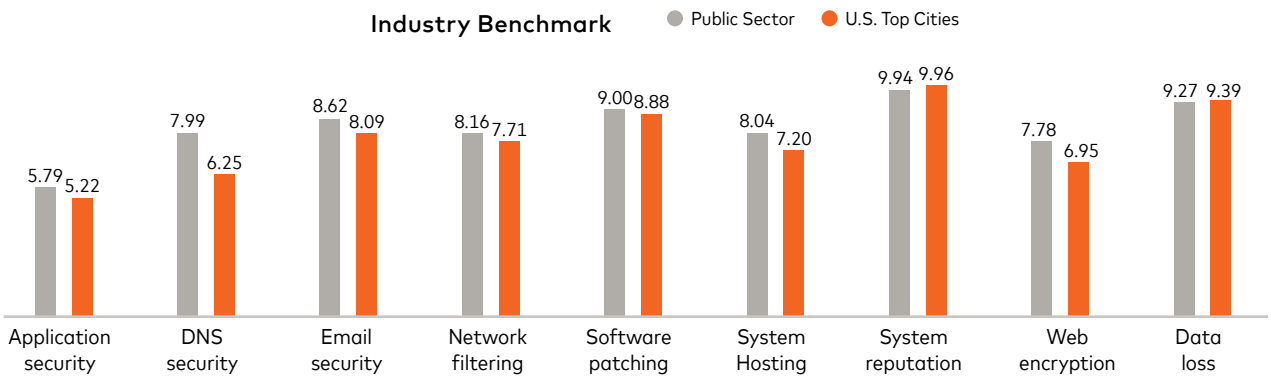
The organizations that RiskRecon monitors within;

- Public Sector Industry have an average rating of 7.7 (B rating)
- Education Industry have an average rating of 7.0 (barely meeting threshold for B rating)
- Finance and Insurance Industry have an average rating above 8.0 (strong B rating)

On security domain performance

RiskRecon evaluates organizations' cyber postures based on their performances across 9 Security Domains. [A detailed description of each domain can be found in **Appendix B**.]

- Top U.S. cities have performed worse than the average Public Sector organization in 7 of the 9 security domains.
- U.S. cities have an average of 26 unique hostnames in their digital ecosystem



Disclaimer: The purpose of this report is to raise awareness about the visible risks and vulnerabilities amongst U.S. cities by illustrating the current cyber risk landscape of the public sector in the context of other industries and geographies. It is not to cast blame or examine the root causes of the current cyber posture of American cities. Many articles and research papers speak to the lack of budgets, difficulties recruiting and maintaining cyber talent, and reliance on legacy infrastructure.

Methodology

For this research, RiskRecon, a Mastercard Company, evaluated a sample of 271 of the most populated U.S. cities' government websites as of August 29, 2021. The sample included the five most populated cities from each state (excluding inhabited territories and including the ten most populated cities for California, Florida, New York, and Texas, and the District of Columbia).

What is RiskRecon?

RiskRecon monitors the cybersecurity performance of an organization using open-source intelligence. RiskRecon employs passive, non-invasive techniques to discover an organization's public systems and analyze those systems' cybersecurity risk posture. RiskRecon summarizes organizational results in an easy-to-understand score called a RiskRecon Rating, which provides a rapid orientation of the organization's cybersecurity performance.

RiskRecon Rating

The RiskRecon Rating is an overall security rating based on performance across 9 Security Domains. RiskRecon rates cybersecurity risk performance on a scale of 0.0 – 10, with 10 being the best rating. RiskRecon overlays an A - F grading scale on top of the numeric ratings that separates performance into five bands. The security domains measured are software patching, application security, web encryption, network filtering, breach events, system reputation, email security, DNS security, and system hosting. [more information on the RiskRecon Rating can be found in **Appendix D**.]

Security Issues

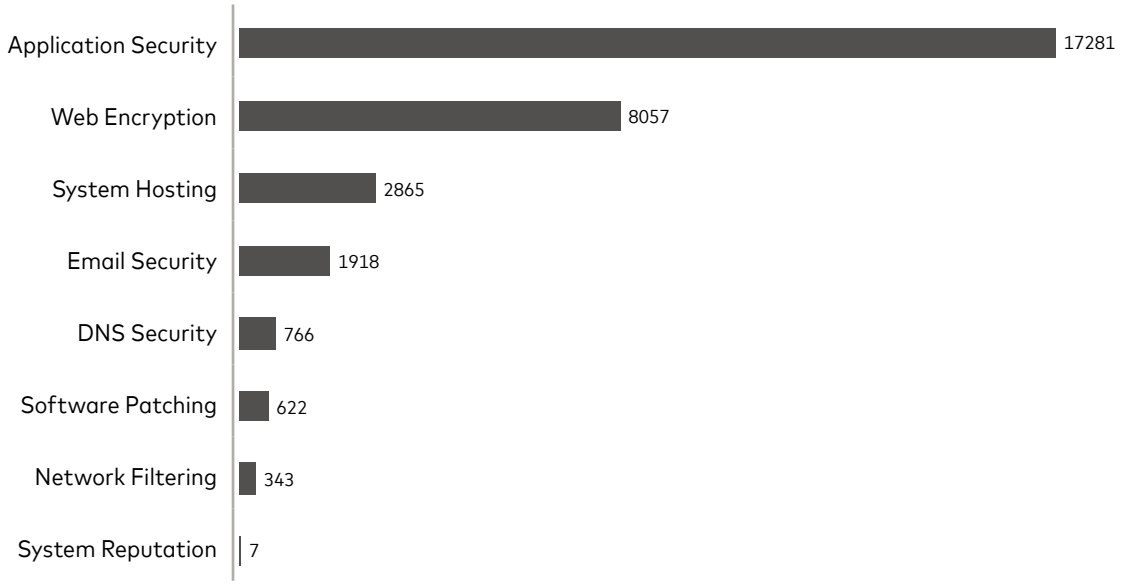
RiskRecon automatically contextualizes every issue with severity and asset value, enabling information security professionals to easily identify risk priorities and needed action. The "priority 1 findings" are issues that are considered critical severity (based on Common Vulnerability Scoring System) discovered on high-valued assets (e.g., a system that collects login information or Personally Identifiable Information).

Security issues and trends

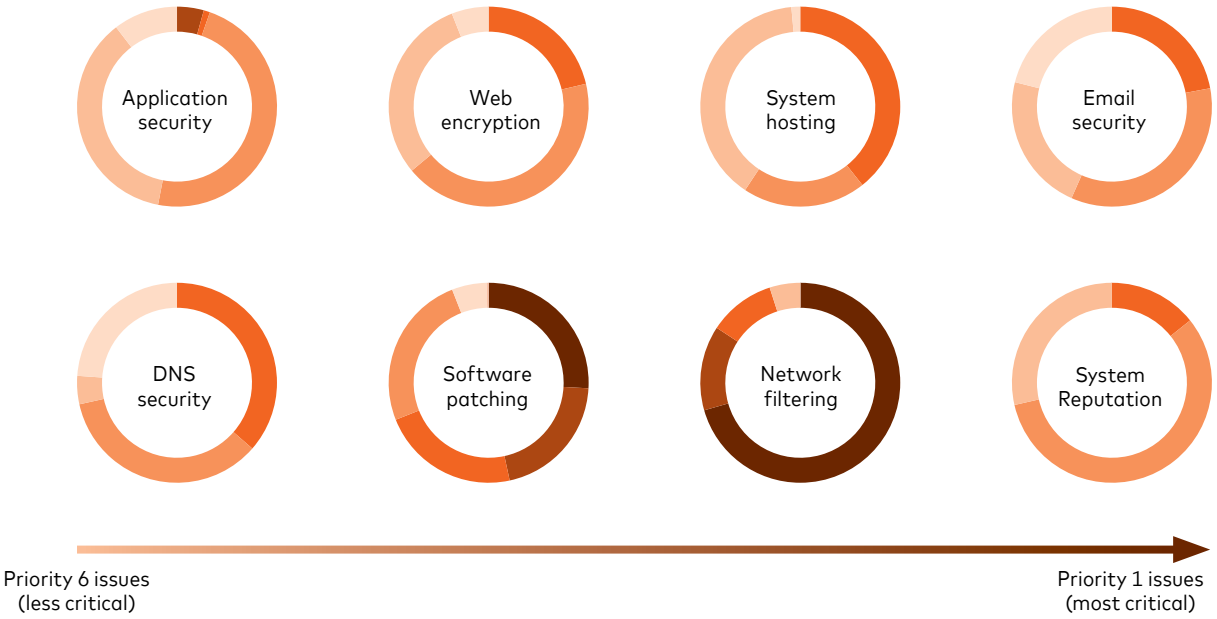
RiskRecon enables organizations to monitor their cybersecurity risks through open-source intelligence techniques. In addition to the alpha-numeric ratings, RiskRecon also identifies specific security issues. These issues are prioritized based on issue severity and asset value. The most severe issues found on the most valuable assets are categorized as "priority 1" issues. [For more details about how RiskRecon prioritizes issues for customers, please refer to **Appendix C**.]

Of the U.S. cities evaluated, RiskRecon identified more than 31,900 cybersecurity issues, of which 403 were considered "priority 1" issues, meaning a critical severity issue on a high-value asset. The Application Security domain accounted for more than half of all identified issues, followed by the Web Encryption and System Hosting Domains. Furthermore, the 110 cities that received a RiskRecon rating of C or below accounted for more than half of all security issues identified and accounted for 80% of the "priority 1" security issues identified.

Security issues by domain



The most frequently observed security issue was missing security headers, accounting for 47% of all findings. Almost all the cities evaluated had at least one occurrence of missing security headers. Other common vulnerabilities included invalid or expired certificate subjects, missing domain hijacking flags, and the use of deprecated or missing encryption protocols. All "priority 1" issues identified involved either the Software Patching or Network Filtering domains. The most common "priority 1" issue found was the use of end-of-life software, which is software that is no longer supported by the vendor and cannot be patched against new or known security issues. The second most common "priority 1" issue was that a system (e.g., a database with sensitive data or a management server) was public-facing and exposed to the internet and should not have been, providing a common vector for cybercriminals to compromise systems and networks.



Of the end-of-life software identified, PHP, Apache, Nginx were the most common products that had reached their end of life and had known security vulnerabilities. These services are widely used in the administration of websites; when left unpatched, they can provide entry points into systems and networks. Additionally, a notable amount of email servers were found to be vulnerable to widespread critical vulnerabilities such as ProxyShell.

When looking at network filtering security issues, 33% of cities evaluated had databases such as MySQL exposed to the internet, leaving sensitive repositories of data potentially accessible to hackers. Another common finding was that more than 10% of cities had Windows computers with Remote Desktop Protocol (RDP) exposed to the internet. RDP has been a frequent target of cybercriminals, and once RDP is exploited, hackers have been known to traverse networks, exfiltrate data, and even deploy ransomware.

Lack of e-mail security was another frequent issue amongst cities. More than 62% of all cities evaluated were not always using e-mail

authentication mechanisms such as Sender Policy Framework (SPF) or Domain Keys Identified Mail (DKIM). Domains that do not implement SPF or DKIM provide no way for other e-mail servers to authenticate the validity of e-mail messages. This provides an opening for fraudsters to send e-mails from unprotected domains, potentially deceiving citizens. Additionally, 14% of cities had domains that did not utilize e-mail encryption to protect the contents of e-mails while in transit.

Beyond the explicit vulnerability findings outlined in our research, cybercriminals often target organizations with poor cybersecurity practices. Criminals may target organizations through social engineering methods such as phishing, which remains an overwhelmingly successful and devastating infiltration method.

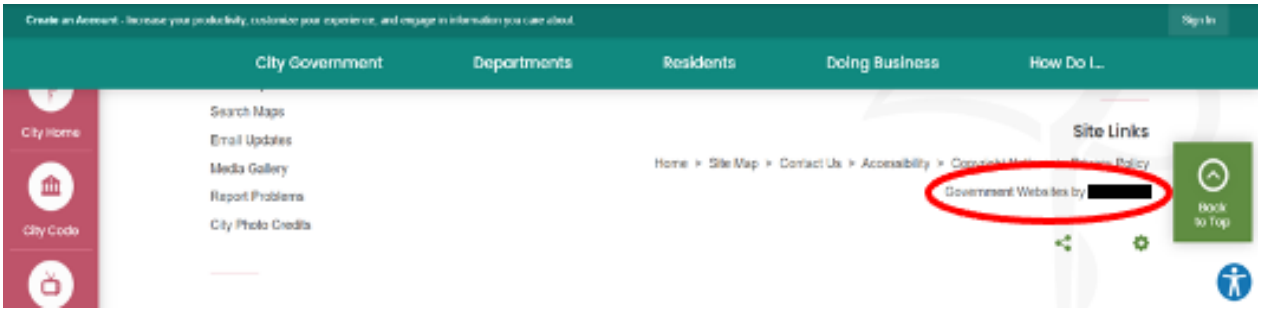
Third-party risk

It is virtually impossible to operate a business, organization, or local government these days without reliance on third parties or third-party tools. While many relationships with third-party entities are publicly visible, others may occur behind the scenes. There is no question, however, that these relationships are crucial for driving day-to-day activities in 2021.

With the increased reliance on third- and fourth-party services comes an increased attack surface and subsequent risk. It's no longer only necessary for organizations to understand their own cybersecurity posture. It is equally important that organizations understand the cybersecurity posture and potential dangers introduced by their third parties.

It is no surprise that articles such as "U.S. cities disclose data breaches after vendor's ransomware attack" and stories involving breaches of vendors leveraged by multiple cities have become regular news items in the past few years. By attacking city vendors, cybercriminals increase the efficiency of their hacks, carrying out "one-to-many" style campaigns where data from constituents across multiple geographies are impacted at once.

In evaluating the 271 cities in our research sample, we visited each city's official website to identify easily observable third parties that were providing website development services. A common theme was that many of the websites visited, 126 (46%) disclosed publicly via the website footer that they were powered or enabled by a third party. While this is just one category of the myriad types of third-party providers with whom local governments typically engage, we chose to use this observation to highlight the dependency on third-party vendors to support everyday operations. Below, we explore select findings on the most observed third-party website development providers, highlighting some of the risks they can introduce and the importance of maintaining a robust third-party risk management program. These risks become even more important to consider when looking at third parties that manage payments, government services, and other essential services on behalf of the city.



We looked further into the cybersecurity posture of the three most prevalent website developers that we observed. The most prevalent website developer provided services for 49 or 18% of the cities evaluated, with the other two most common providers supporting an additional 31 cities. We then analyzed and stratified the assessments of cities by their website developer.

Our analysis showed that the average RiskRecon rating and performance across our nine security domains varied significantly depending on a city's website developer. While the highest performing group of cities (when grouped by website developer) had an average RiskRecon rating of 7.9 (a B rating), the worst-performing cities associated with a specific website developer only scored 7.0 (barely meeting the threshold for a B rating). This trend continued across most security domains, and we found that the security performance of the worst-performing group of cities had an average of 3.73 "priority 1" issues in their portfolio compared to an average of 1.55 "priority 1" issues across all 271 cities. Furthermore, the same low-performing group of cities had an average of 130 security findings per city compared to an average of 85 security findings among the cities developed by the three prevalent providers. Perhaps most startling is that the same group of cities suffered nearly 40% more breach events when compared to all 271 cities.

Conclusion: staying protected

The cybersecurity conditions going into 2022 are a perfect combination that will lead to the hardest year the world has ever faced in ensuring the confidentiality, integrity, and availability of systems and data. Leading into 2022, criminals have dramatically improved the scalability and effectiveness of their cybercrime and ransomware operations. Thus, having a cybersecurity risk monitoring program for one's own organization as well as having one for third parties is more important than ever.

RiskRecon helps organizations understand and act on their third and fourth-party cyber risk by providing easy-to-comprehend cybersecurity risk ratings, enabling organizations to confidently make better risk decisions - faster.

As a leading provider of cybersecurity ratings, RiskRecon continuously monitors the cybersecurity risk of over 15 million companies across the most highly regulated industries from finance and insurance to aerospace and healthcare. RiskRecon provides deep, risk-contextualized, data-driven insights into the security risk performance across a customer's entire ecosystem and helps pinpoint specific gaps in any organization's security programs and performance.

Our unique risk-prioritized action plans rely on advanced models and analytics to prioritize findings by asset value and issue severity. RiskRecon is the only continuous cyber risk ratings and insights tool with its own security measurements model, comprised of more than 40 unique criteria, providing you with the most accurate, deep, and broad picture of your organization's cyber risk.

For more information on how to leverage RiskRecon to manage your organization's cyber risk posture at scale, request a demo at riskrecon.com

Appendix A – Dataset

The dataset includes the domains of the top five most populous cities in each of the 50 United States, as of August 29, 2021. The data also includes the District of Columbia and has been expanded to include the top ten most populous cities in New York, California, and Texas.

- In some instances, based on governance structure, cities were evaluated at the county level.

State	City	Domain
Alabama	Birmingham	www.birminghamal.gov
Alabama	Huntsville	www.huntsvilleal.gov
Alabama	Montgomery	www.montgomeryal.gov
Alabama	Mobile	www.cityofmobile.org
Alabama	Tuscaloosa	www.tuscaloosa.com
Alaska	Anchorage	www.muni.org
Alaska	Juneau	www.juneau.org
Alaska	Fairbanks	www.fairbanksalaska.us
Alaska	Wasilla	www.cityofwasilla.com
Alaska	Sitka	www.cityofsitka.com
Arizona	Phoenix	www.phoenix.gov
Arizona	Tucson	www.tucsonaz.gov
Arizona	Mesa	www.mesaaz.gov
Arizona	Chandler	www.chandleraz.gov
Arizona	Scottsdale	www.scottsdaleaz.gov
Arkansas	Little Rock	www.littlerock.gov
Arkansas	Fort Smith	www.fortsmithar.gov
Arkansas	Fayetteville	www.fayetteville-ar.gov
Arkansas	Springdale	www.springdalear.gov
Arkansas	Jonesboro	www.jonesboro.org
California	Los Angeles	www.lacity.org
California	San Diego	www.sandiego.gov
California	San Jose	www.sanjoseca.gov
California	San Francisco	www.sf.gov
California	Fresno	www.fresno.gov
California	Sacramento	www.cityofsacramento.org
California	Long Beach	www.longbeach.gov
California	Oakland	www.longbeach.gov
California	Bakersfield	www.bakersfieldcity.us
California	Anaheim	www.anaheim.net
Colorado	Denver	www.denvergov.org

Colorado	Colorado Springs	www.coloradosprings.gov
Colorado	Aurora	www.auroragov.org
Colorado	Fort Collins	www.fcgov.com
Colorado	Lakewood	www.lakewood.org
Connecticut	Bridgeport	www.bridgeportct.gov
Connecticut	New Haven	www.newhavenct.gov
Connecticut	Stamford	www.stamfordct.gov
Connecticut	Hartford	www.hartfordct.gov
Connecticut	Waterbury	www.waterburyct.org
Delaware	Wilmington	www.wilmingtonde.gov
Delaware	Dover	www.cityofdover.com
Delaware	Newark	www.newarkde.gov
Delaware	Middletown	www.middletown.delaware.gov
Delaware	Smyrna	www.smyrna.delaware.gov
District of Columbia	Washington, D.C.	www.dc.gov
Florida	Jacksonville	www.coj.net
Florida	Miami	www.miamigov.com
Florida	Tampa	www.tampa.gov
Florida	Orlando	www.orlando.gov
Florida	St. Petersburg	www.stpete.org
Florida	Hialeah	www.hialeahfl.gov
Florida	Tallahassee	www.talgov.com
Florida	Port St. Lucie	www.cityofpsl.com
Florida	Cape Coral	www.capecoral.net
Florida	Fort Lauderdale	www.fortlauderdale.gov
Georgia	Atlanta	www.atlantaga.gov
Georgia	Augusta	www.augustaga.gov
Georgia	Columbus	www.columbusga.gov
Georgia	Macon	www.maconbibb.us
Georgia	Savannah	www.savannahga.gov
Hawaii	Honolulu	www.honolulu.gov
Hawaii	East Honolulu	www.honolulu.gov
Hawaii	Pearl City	www.honolulu.gov
Hawaii	Hilo	www.hawaiicounty.gov
Hawaii	Kailua	www.kailuatownhi.com
Idaho	Boise	www.cityofboise.org
Idaho	Meridian	www.meridiancity.org
Idaho	Nampa	www.cityofnampa.us

Idaho	Idaho Falls	www.idahofallsidaho.gov
Idaho	Caldwell	www.cityofcaldwell.org
Illinois	Chicago	www.chicago.gov
Illinois	Aurora	www.aurora-il.org
Illinois	Naperville	www.naperville.il.us
Illinois	Joliet	www.joliet.gov
Illinois	Rockford	www.rockfordil.gov
Indiana	Indianapolis	www.indy.gov
Indiana	Fort Wayne	www.cityoffortwayne.org
Indiana	Evansville	www.evansvillegov.org
Indiana	South Bend	www.southbendin.gov
Indiana	Carmel	www.carmel.in.gov
Iowa	Des Moines	www.dsm.city
Iowa	Cedar Rapids	www.cedar-rapids.org
Iowa	Davenport	www.davenportiowa.com
Iowa	Sioux City	www.sioux-city.org
Iowa	Iowa City	www.icgov.org
Kansas	Wichita	www.wichita.gov
Kansas	Overland Park	www.opkansas.org
Kansas	Kansas City	www.kcmo.gov
Kansas	Olathe	www.olatheks.org
Kansas	Topeka	www.topeka.org
Kentucky	Louisville	www.louisvilleky.gov
Kentucky	Lexington	www.lexingtonky.gov
Kentucky	Bowling Green	www.bgky.org
Kentucky	Owensboro	www.owensboro.org
Kentucky	Covington	www.covingtonky.gov
Louisiana	New Orleans	www.nola.gov
Louisiana	Baton Rouge	www.brla.gov
Louisiana	Shreveport	www.shreveportla.gov
Louisiana	Lafayette	www.lafayettela.gov
Louisiana	Lake Charles	www.cityoflakecharles.com
Maine	Portland	www.portlandmaine.gov
Maine	Lewiston	www.lewistonmaine.gov
Maine	Bangor	www.bangormaine.gov
Maine	South Portland	www.southportland.org
Maine	Auburn	www.auburnmaine.gov
Maryland	Baltimore	www.baltimorecity.gov

Maryland	Columbia	www.howardcountymd.gov
Maryland	Germantown	www.montgomerycountymd.gov
Maryland	Silver Spring	www.montgomerycountymd.gov
Maryland	Waldorf	www.charlescountymd.gov
Massachusetts	Boston	www.boston.gov
Massachusetts	Worcester	www.worcesterma.gov
Massachusetts	Springfield	www.springfield-ma.gov
Massachusetts	Cambridge	www.cambridgema.gov
Massachusetts	Lowell	www.lowellma.gov
Michigan	Detroit	www.detroitmi.gov
Michigan	Grand Rapids	www.grandrapidsmi.gov
Michigan	Warren	www.cityofwarren.org
Michigan	Sterling Heights	www.sterling-heights.net
Michigan	Ann Arbor	www.a2gov.org
Minnesota	Minneapolis	www.minneapolismn.gov
Minnesota	Saint Paul	www.stpaul.gov
Minnesota	Rochester	www.rochestermn.gov
Minnesota	Duluth	www.duluthmn.gov
Minnesota	Bloomington	www.bloomingtonmn.gov
Mississippi	Jackson	www.jacksonms.gov
Mississippi	Gulfport	www.gulfport-ms.gov
Mississippi	Southaven	www.southaven.org
Mississippi	Biloxi	www.biloxi.ms.us
Mississippi	Hattiesburg	www.hattiesburgms.com
Missouri	Kansas City	www.kcmo.gov
Missouri	Saint Louis	www.stlouis-mo.gov
Missouri	Springfield	www.springfieldmo.gov
Missouri	Columbia	www.como.gov
Missouri	Independence	www.ci.independence.mo.us
Montana	Billings	www.ci.billings.mt.us
Montana	Missoula	www.ci.missoula.mt.us
Montana	Great Falls	www.greatfallsmt.net
Montana	Bozeman	www.bozeman.net
Montana	Butte	www.co.silverbow.mt.us
Nebraska	Omaha	www.cityofomaha.org
Nebraska	Lincoln	www.lincoln.ne.gov
Nebraska	Bellevue	www.bellevue.net
Nebraska	Grand Island	www.grand-island.com

Nebraska	Kearney	www.cityofkearney.org
Nevada	Las Vegas	www.lasvegasnevada.gov
Nevada	Henderson	www.cityofhenderson.com
Nevada	Reno	www.reno.gov
Nevada	North Las Vegas	www.cityofnorthlasvegas.com
Nevada	Paradise	www.clarkcountynv.gov
New Hampshire	Manchester	www.manchesternh.gov
New Hampshire	Nashua	www.nashuanh.gov
New Hampshire	Concord	www.concordnh.gov
New Hampshire	Dover	www.dover.nh.gov
New Hampshire	Rochester	www.rochesternh.net
New Jersey	Newark	www.newarknj.gov
New Jersey	Jersey City	www.jerseycitynj.gov
New Jersey	Paterson	www.patersonnj.gov
New Jersey	Elizabeth	www.elizabethnj.org
New Jersey	Edison	www.edisonnj.org
New Mexico	Albuquerque	www.cabq.gov
New Mexico	Las Cruces	www.las-cruces.org
New Mexico	Rio Rancho	www.rrnm.gov
New Mexico	Santa Fe	www.santafenm.gov
New Mexico	Roswell	www.roswell-nm.gov
New York	New York City	www.nyc.gov
New York	Buffalo	www.buffalony.gov
New York	Rochester	www.cityofrochester.gov
New York	Yonkers	www.yonkersny.gov
New York	Syracuse	www.syrgov.net
New York	Albany	www.albanyny.gov
New York	New Rochelle	www.newrochelleny.com
New York	Cheektowaga	www.tocny.org
New York	Mount Vernon	www.cmvny.com
New York	Schenectady	www.cityofschenectady.com
North Carolina	Charlotte	www.charlottenc.gov
North Carolina	Raleigh	www.raleighnc.gov
North Carolina	Greensboro	www.greensboro-nc.gov
North Carolina	Durham	www.durhamnc.gov
North Carolina	Winston-Salem	www.cityofws.org
North Dakota	Fargo	www.fargond.gov
North Dakota	Bismarck	www.bismarcknd.gov

North Dakota	Grand Forks	www.grandforksgov.com
North Dakota	Minot	www.minotnd.org
North Dakota	West Fargo	www.westfargond.gov
Ohio	Columbus	www.columbus.gov
Ohio	Cleveland	www.clevelandohio.gov
Ohio	Cincinnati	www.cincinnati-oh.gov
Ohio	Toledo	www.toledo.oh.gov
Ohio	Akron	www.akronohio.gov
Oklahoma	Oklahoma City	www.okc.gov
Oklahoma	Tulsa	www.cityoftulsa.org
Oklahoma	Norman	www.normanok.gov
Oklahoma	Broken Arrow	www.brokenarrowok.gov
Oklahoma	Edmond	www.edmondok.com
Oregon	Portland	www.portland.gov
Oregon	Salem	www.cityofsalem.net
Oregon	Eugene	www.eugene-or.gov
Oregon	Gresham	www.greshamoregon.gov
Oregon	Hillsboro	www.hillsboro-oregon.gov
Pennsylvania	Philadelphia	www.phila.gov
Pennsylvania	Pittsburgh	www.pittsburghpa.gov
Pennsylvania	Allentown	www.allentownpa.gov
Pennsylvania	Erie	www.eriecountypa.gov
Pennsylvania	Reading	www.readingpa.gov
Rhode Island	Providence	www.providenceri.gov
Rhode Island	Cranston	www.cranstonri.gov
Rhode Island	Warwick	www.warwickri.gov
Rhode Island	Pawtucket	www.pawtucketri.com
Rhode Island	East Providence	www.eastprovidenceri.gov
South Carolina	Charleston	www.charleston-sc.gov
South Carolina	Columbia	www.columbiasc.net
South Carolina	North Charleston	www.northcharleston.org
South Carolina	Mount Pleasant	www.tompsc.com
South Carolina	Rock Hill	www.cityofrockhill.com
South Dakota	Sioux Falls	www.siouxfalls.org
South Dakota	Rapid City	www.rcgov.org
South Dakota	Aberdeen	www.aberdeen.sd.us
South Dakota	Brookings	www.cityofbrookings-sd.gov
South Dakota	Watertown	www.watertownsd.us

Tennessee	Nashville	www.nashville.gov
Tennessee	Memphis	www.memphistn.gov
Tennessee	Knoxville	www.knoxvilletn.gov
Tennessee	Chattanooga	www.chattanooga.gov
Tennessee	Clarksville	www.cityofclarksville.com
Texas	Houston	www.houstontx.gov
Texas	San Antonio	www.sanantonio.gov
Texas	Dallas	www.dallascityhall.com
Texas	Austin	www.austintexas.gov
Texas	Fort Worth	www.fortworthtexas.gov
Texas	El Paso	www.elpasotexas.gov
Texas	Arlington	www.arlingtontx.gov
Texas	Corpus Christi	www.cctexas.com
Texas	Plano	www.plano.gov
Texas	Laredo	www.cityoflaredo.com
Utah	Salt Lake City	www.slc.gov
Utah	West Valley City	www.wvc-ut.gov
Utah	Provo	www.provo.org
Utah	West Jordan	www.westjordan.utah.gov
Utah	Orem	www.orem.org
Vermont	Burlington	www.burlingtonvt.gov
Vermont	South Burlington	www.southburlingtonvt.gov
Vermont	Rutland	www.rutlandcity.org
Vermont	Barre	www.barrecity.org
Vermont	Montpelier	www.montpelier-vt.org
Virginia	Virginia Beach	www.vbgov.com
Virginia	Norfolk	www.norfolk.gov
Virginia	Chesapeake	www.cityofchesapeake.net
Virginia	Richmond	www.rva.gov
Virginia	Newport News	www.nnva.gov
Washington	Seattle	www.seattle.gov
Washington	Spokane	www.my.spokanecity.org
Washington	Tacoma	www.cityoftacoma.org
Washington	Vancouver	www.cityofvancouver.us
Washington	Bellevue	www.bellevuewa.gov
West Virginia	Charleston	www.charlestonwv.gov
West Virginia	Huntington	www.cityofhuntington.com
West Virginia	Morgantown	www.morgantownwv.gov

West Virginia	Parkersburg	www.parkersburgcity.com/pc
West Virginia	Wheeling	www.wheelingwv.gov
Wisconsin	Milwaukee	www.city.milwaukee.gov
Wisconsin	Madison	www.cityofmadison.com
Wisconsin	Green Bay	www.greenbaywi.gov
Wisconsin	Kenosha	www.kenosha.org
Wisconsin	Racine	www.cityofracine.org
Wyoming	Cheyenne	www.cheyennecity.org
Wyoming	Casper	www.casperwy.gov
Wyoming	Laramie	www.cityoflaramie.org
Wyoming	Gillette	www.gillettewy.gov
Wyoming	Rock Springs	www.rswy.net

Appendix B – Security Domains

Application Security

The application security domain assesses each web application for essential, observable application security practices that are leading indicators of the quality of the application security program.

DNS Security

The DNS Security domain assesses the use of controls to prevent unauthorized modification of domain records resulting in domain hijacking. This domain also enumerates the DNS hosting providers to determine level of fragmentation. Control of DNS records is essential to keeping systems accessible. Where domain hijacking controls do not appear to be implemented, the organization should demonstrate compensating controls or implement the recommended domain protection settings.

E-mail Security

The email security domain assesses the use of authentication and encryption controls necessary to ensure that email messages are not spoofed and that communications are private. The domain also enumerates the email hosting providers, providing visibility into the email hosting providers. Organizations should consistently implement email encryption for all servers and email authentication for all domains. Where the organization has a high number of email hosting providers, the organization should be asked to explain how they defend email bourn threats emanating through each provider system.

Network Filtering

The domain enumerates unsafe network services and Internet of Things (IoT) devices the organization has exposed to the internet. Enterprises should limit Internet-accessible network services and systems to those that are safe and necessary. Unsafe network services and IoT devices are very susceptible to compromise through various methods such as credential guessing, communications intercept, and vulnerability exploitation. RiskRecon analyzes Internet-facing systems and networks for the following services: MS SQL Server, MySQL, PostgreSQL, MongoDB, Elastic, DB2, Redis, Memcached, CouchDB, Cassandara, Remote Desktop Protocol, VNC, Telnet, FTP, Samba, Finger, NetBIOS, BGP, PPTP, X11, Oracle TNS, Apple Airport, Webmin. RiskRecon analyzes systems and networks to discover Internet of Things (IoT) devices, such as printers, elevator control systems, HVAC interfaces, cameras, and network storage devices.

Software Patching

The domain enumerates systems that are running end of life and vulnerable software. Because end of life software is not supported by the vendor, it cannot be patched against known security issues or new vulnerabilities that might be discovered. All software patching issues should be addressed immediately, and software patching practices should be modified to ensure that software remains current going forward. Further details are provided in the downloadable software data file.

System Hosting

The domain analyzes the hosting practices of the organization, enumerating the hosting providers and the countries that systems are hosted in. It is essential to ensure that systems are hosted in reputable countries and that the host country data privacy laws are obeyed. High fragmentation of hosting with a large number of hosting providers is a leading indicator of gaps in I.T. governance.

System Reputation

RiskRecon analyzed I.P. reputation and threat intelligence databases to identify suspicious system activity. Observed malicious activity may indicate the system is compromised or is being used for unauthorized purposes. Of the issues identified, Mastercard - Sandbox selected those detailed in this section as important to investigate and address due to the issue severity and the sensitivity of the system in which the issue exists.

Web Encryption

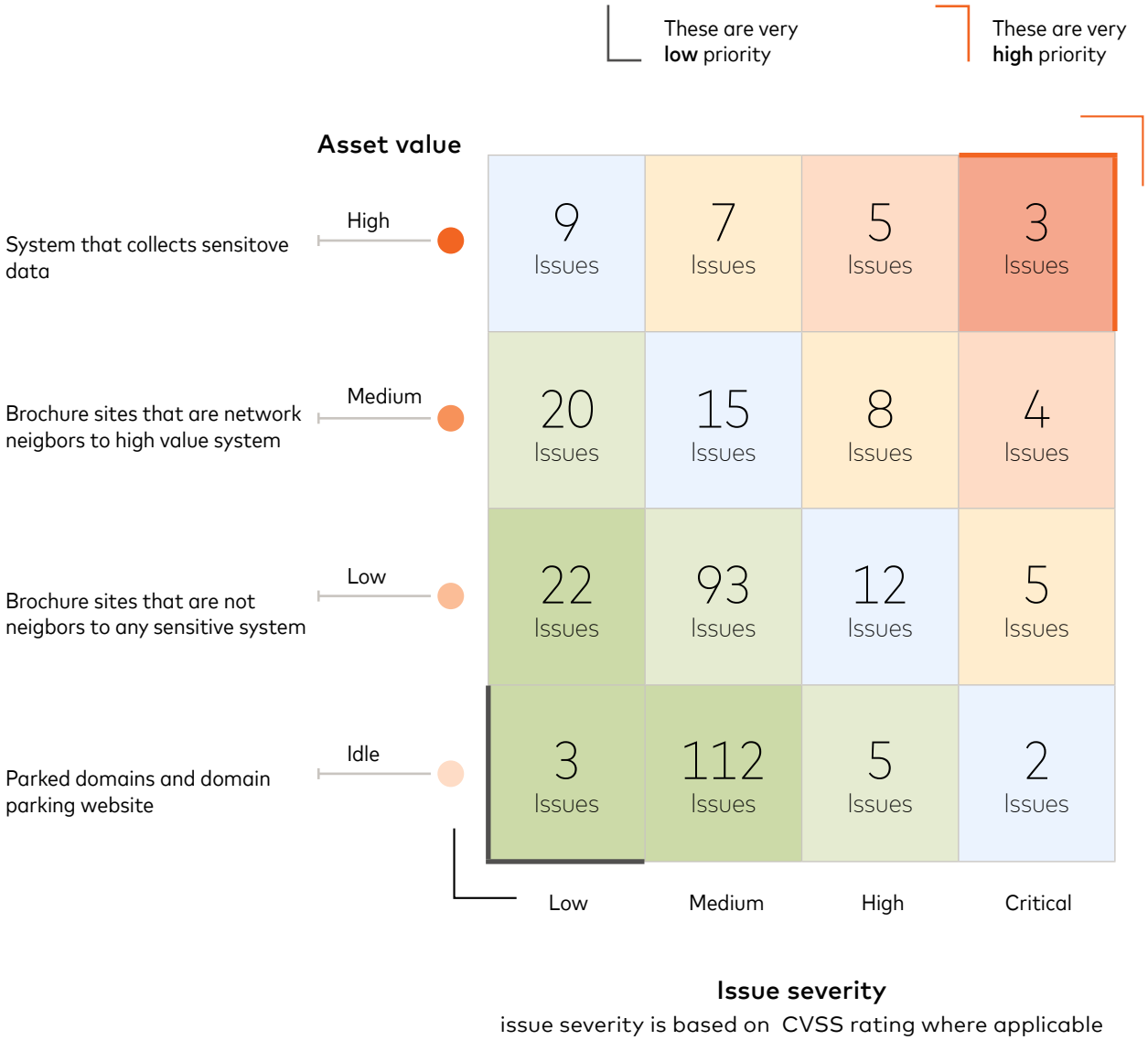
The domain analyzes the effectiveness of encryption implementations, determining if they are properly configured to prevent errors, use secure protocols and apply minimum key lengths necessary to ensure communication privacy. All encryption errors should be addressed to prevent encryption errors being displayed to users and to ensure that the encryption implementation is effective.

Breach Events

The domain summarizes the breach events the organization has experienced. Recent breach events indicate gaps in the breach protection program. Organizations with breach events occurring consistently over time likely have ineffective breach prevention programs and material gaps in their information security program. Organizations with recent and repeated breach events over time should be examined closely to ensure that controls are operating effectively to prevent future breaches and loss of data.

Appendix C – Security Issue Findings

RiskRecon risk prioritizes every issue based on the severity of the issue and the value of the asset in which the issue exists. RiskRecon uses the Issue Priority Matrix to visualize risk. Issues become increasingly severe from left to right of the matrix, and assets become more and more value from bottom to top. Issues in the top right quadrant are the most severe ones found on higher-value assets, which need immediate attention and a quick fix. On the contrary, issues in the bottom left quadrant are the less severe ones found on lower-value assets, which should be evaluated but may not require an immediate fix.



Appendix D – RiskRecon Rating

RiskRecon rates the quality of enterprise cybersecurity risk performance based on continuous collection and analytics of open-source intelligence signals that determine the rates and severities of cybersecurity issues within the context of the value at risk of the systems in which the issues exist. RiskRecon's risk assessment scope spans nine security domains built on approximately 40 criteria which assess systems against thousands of security tests.

Rating Scale	
Grade	**Rating Range**
A	8.5–10
B	7.0–8.4
C	5.5–6.9
D	4.0–5.4
F	0.0–3.9

RiskRecon rates cybersecurity risk performance on a scale of 0.0–10, with 10 being the best rating. RiskRecon overlays an A-F grading scale on top of the numeric ratings that separates performance into five bands. RiskRecon selected the five-tier grading system for two reasons. First, the A–F grading system is internationally familiar, with Wikipedia showing that at least 37 countries use the system for grading student performance. This aids consumers of the ratings in quickly understanding their own performance in relation to other companies. Second, five tiers provide useful portfolio-level performance segmentation, making it easier for analysts to identify and act on portfolio risk hot spots.

Have comments or questions about this report?

Contact RiskRecon at info@riskrecon.com or @riskrecon on Twitter

riskrecon

mastercard

Designed by Creative Studio

RiskRecon enables organizations to quickly understand and act on their third and fourth-party risk through prioritized and easy-to-understand cybersecurity ratings and insights.

www.riskrecon.com