charlesworth consulting

1828 WALNUT STREET, SUITE 701
KANSAS CITY, MO 64108
(913) 851.4730
CHARLESWORTHCONSULTING.COM

Responding to Ransomware Attacks

Average and Median Ransom Payment Amounts Declined in Q2 2021

Average Ransom Payment

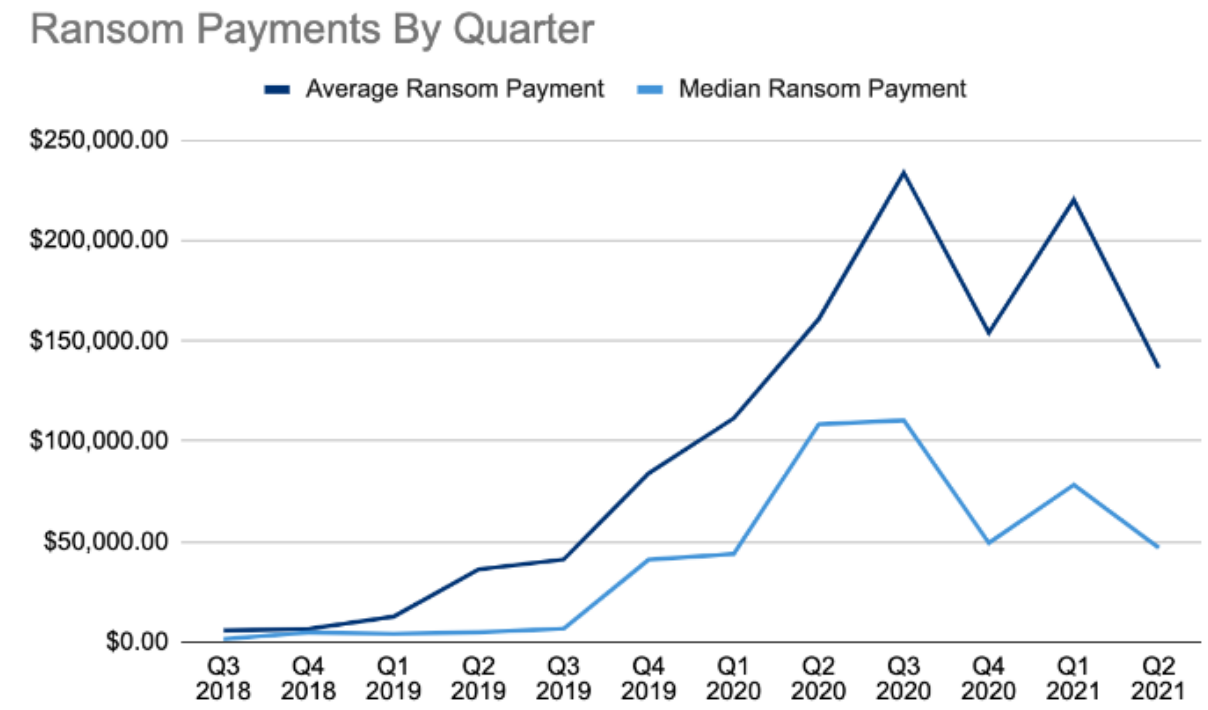
$136,576

-38% from Q1 2021

Median Ransom Payment

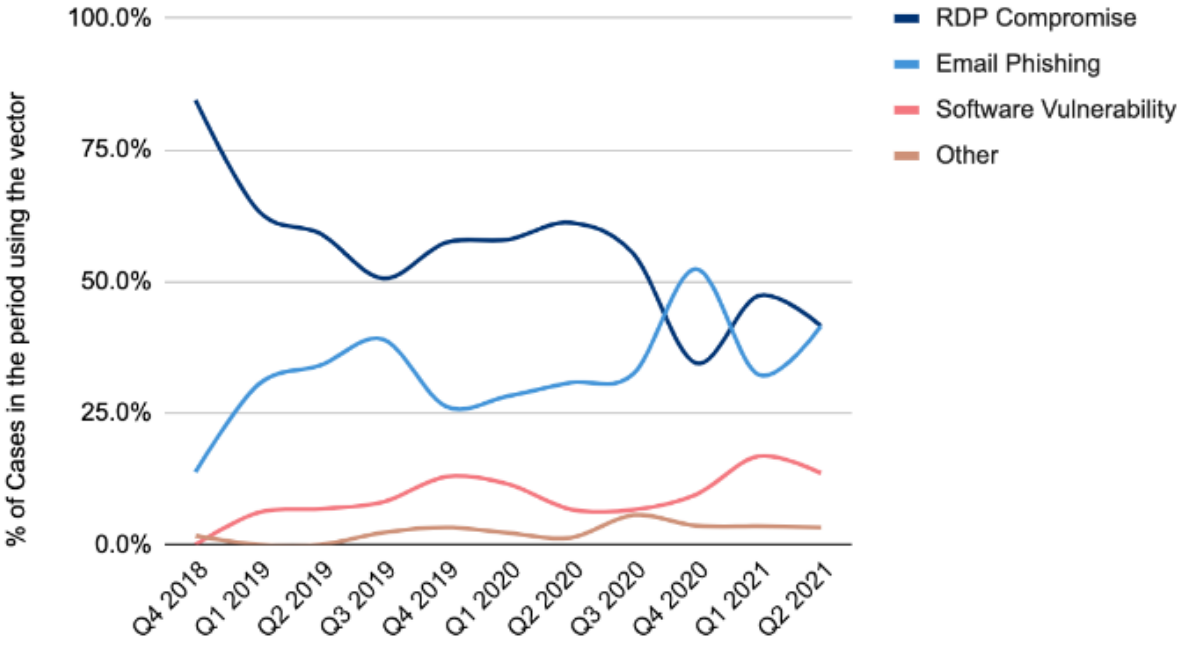
$47,008

-40% from Q1 2021



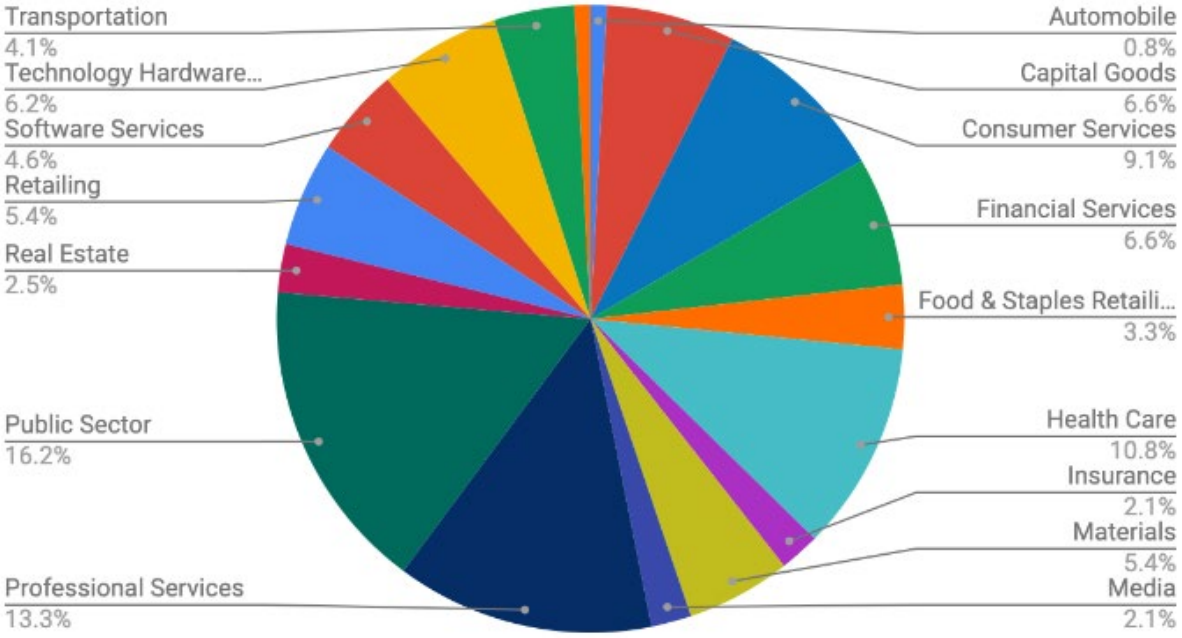
COVEWARE

Ransomware Attack Vectors



COVEWARE

Common Industries Targeted by Ransomware Q2 2021



COVEWARE

Profile of a Typical Ransomware Attack

A typical ransomware attack involves three distinct phases:

1. **Gaining persistence**: A threat actor gains access to the network of an organization. There are several common vectors through which persistence on the network is achieved (to be discussed later). Regardless of the means by which access is achieved, threat actors will typically elevate themselves to administrative user privileges, allowing them to move freely through the network and control critical systems like domain controllers, anti-virus protection, endpoint protection, authentication, and the back-up systems. During this phase, the actor may attempt to steal banking passwords (so they can be monetized separately) and exfiltrate sensitive data (for further sale to third parties or to add leverage in the extortion). They will map the network and develop a plan to encrypt it.

2. **Detonation**: After sufficient time surveilling and exfiltrating data, the last step is the detonation of the ransomware. The threat actors will turn off antivirus and endpoint protection, which essentially cuts the alarms that would otherwise alert the company. They will delete or encrypt the organization's backup systems. This cripples the company's ability to restore their network quickly. Finally the threat actors will fully encrypt the primary servers and computers of the company. Once the encryption is finished, ransom notes are left on every machine of the organization. They then wait to be contacted.

3. **Extortion**: If the organization has not properly segmented or air gapped their backups, they are effectively crippled. The organization's email is likely inoperable. Their website may be down. Enterprise Resource Planning application systems that control billing, payroll, shipping and other critical functions may be crippled, and phone systems may also be down. Most organizations have to resort to some form of paper and pencil operations if they are truly crippled to this extent. If the degree of interruption threatens the viability of the company, they face two terrible choices: i) choose to lose their customers, dismiss their employees and possibly close their company, or ii) negotiate and pay the ransom demanded by the threat actors. This is the exact choice thousands of organizations are faced with every year. When victims choose to pay a ransom in cryptocurrency to the threat actor, the threat actor may provide a decryption key, though the efficacy of the decryption key can vary between threat actor groups as does the likelihood of receiving the key.

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
Alabama	Ala. Code § 8-38-3	The state, a county or a municipality or instrumentality of same and third-party agents.	Implement and maintain reasonable security measures to protect sensitive personally identifying information as specified.
Arizona	Ariz. Rev. Stat. § 18-105	State budget units and state agencies	Establishes a statewide information security and privacy office. Provides that the office serve as the strategic planning, facilitation and coordination office for information technology security in the state. Individual budget units continue to maintain operational responsibility for information technology security. Provides for the appointment of a statewide chief information security officer to manage the statewide information security and privacy office. Requires the office to direct security and privacy compliance reviews, identify and mitigate security and privacy risks, monitor compliance with policies and standards, and coordinate training programs.
California	Calif. Govt. Code § 11549.3 et seq.	State agencies.	Comply with information security program developed by the Chief of the Office of Information Security, as

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
	Calif. Govt. Code § 8592.30-8592.45 Calif. Govt. Code § 8586.5		specified/detailed in statute, including conducting an annual independent security assessment. Requires each state agency to implement cybersecurity strategy incident response standards to secure its critical infrastructure controls and critical infrastructure information. Establishes the California Cybersecurity Integration Center (Cal-CSIC) to develop a statewide cybersecurity strategy. Requires Cal-CSIC to establish a cyber incident response team and directs all state departments and agencies to comply with information security and privacy policies and to promote awareness of information security standards with their workforce.
Colorado	C.R.S. §§ 24-37.5-403, -404, -404.5, -405	Public agencies, institutions of higher education, General Assembly	Requires the chief information security officer to: (a) Develop and update information security policies,

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			standards, and guidelines for public agencies; (b) Promulgate rules pursuant to article 4 of this title containing information security policies, standards, and guidelines; (c) Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies pursuant to *section 24-37.5-404*; (d) Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments. Establishes the Colorado Cybersecurity Council and provides for coordination of missions related to homeland security and cybersecurity. Requires public agencies and institutions of higher education to develop an information security plan utilizing the information security policies, standards, and guidelines developed by the chief information security

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			officer. Provides for an information security plan for communication and information resources that support the operations and assets of the general assembly Encourages the CISO to assess the data systems of each public agency for the benefits and costs of adopting and applying distributed ledger technologies such as blockchains.
Connecticut	C.G.S. § 4e-70	Any state agency with a department head and any state agency disclosing confidential information to a contractor pursuant to a written agreement with such contractor for the provision of goods or services for the state.	Implement and maintain a comprehensive data-security program for the protection of confidential information. The Secretary of the Office of Policy and Management, or the secretary's designee, may require additional protections or alternate measures of security assurance when warranted.
Delaware	29 Del. Code § 9011C	State agencies	Provides that the Department of Technology and Information may develop and implement a comprehensive information security program that applies personnel,

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			process, and technology controls to protect the state's data, systems, and infrastructure. The department also shall identify and address information security risks to each State agency, to third-party providers, and to key supply chain partners. Provides for a central Security Operations Center to direct statewide cyber defense and cyber threat mitigation. Implements technical compliance to state-owned technology as required by law or as recommended by private industry standards. Allows the department to temporarily disrupt the exposure of an information system or information technology infrastructure that is owned, leased, outsourced, or shared by one or more state agencies in order to isolate the source of, or stop the spread of, an information security breach or other similar information security incident.
Florida	Fla. Stat. § 282.318**,**	State agencies.	Comply with the statewide information technology

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
	Fla. Stat. § 20.61		security standards and processes developed by the Agency for State Technology as specified/detailed in statute, including conducting and updating a comprehensive risk assessment every three years, creating an incident response team and reporting process, and providing security and cybersecurity awareness training for all state agency employees.
Georgia	Georgia Code § 50-25-4	Agencies	The Georgia Technology Authority shall have the following powers (21) To establish technology security standards and services to be used by all agencies; (22) To conduct technology audits of all agencies;
Idaho	Idaho Code §§ 67-827, 67-827A	State agencies	Creates the office of information technology services (OITS) within the office of the governor. Designates the administrator of OITS to oversee all information technology services and cybersecurity policies within the state. This includes the coordination and implementation of

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			cybersecurity policies, information security needs, tests and vulnerability scans to mitigate risks and mandatory education and training of state employees.
Illinois	20 ILCS 1375/Art. 5 30 ILCS 5/3-2.4	State agencies	Establishes the Office of Statewide Chief Information Security Officer to serve as the strategic planning, facilitation and coordination office for information technology security in the state. Provides services to support agencies, such as identifying risks through assessments, coordinating statewide information security awareness and training programs, among other responsibilities specified/detailed in statute. Cybersecurity audit. Requires the Auditor General to review state agencies and their cybersecurity programs and practices, with a particular focus on agencies holding large volumes of personal information.
Indiana	Ind. Code § 4-13.1-2-2	State agencies	The Office Of Technology shall

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			(9) Review projects, architecture, security, staffing, and expenditures. (10) Develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government. (11) Advise the state personnel department on guidelines for information technology staff for state agencies. (12) Conduct periodic management reviews of information technology activities within state agencies upon request.
Kansas	Kan. Stat. § 75-7240	Executive branch agencies	Requires executive branch agency heads to ensure that information security programs are in place, implement security policies, standards and cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources; include cybersecurity requirements in agency request for proposal specifications for procuring data and information

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			technology systems and services; submit a cybersecurity assessment report to the CISO by October 16 of each even-numbered year, and other requirements as specified in statute.
Kentucky	K.R.S. § 42-724 K.R.S. § 61.932(1)	Public agencies and nonaffiliated third parties.	An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches. Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology.

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
Maryland	Md. State Govt. Code §§ 10-1301, -1304	An executive agency, a department, a board, a commission, an authority, a public institution of higher education, a unit or an instrumentality of the State; or a county, municipality, bi–county, regional, or multicounty agency, county board of education, public corporation or authority, or any other political subdivision of the State.	Implement and maintain a written information security policy and reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations. Require, by written contract or agreement, that third parties implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information disclosed to the nonaffiliated third party.
Massachusetts	Mass. Gen. Laws Ch. 93H § 2(c)	The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor.	Adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
Minnesota	Minn. Stat. § 16E.03	State agencies in the executive branch of state government, including the Minnesota Office of Higher Education, but not the Minnesota State Colleges and Universities.	Provides that the chief information officer (CIO) shall establish and enforce standards and ensure acquisition of hardware and software necessary to protect data and systems in state agency networks connected to the Internet. Further provides that the CIO shall establish cyber security policies, guidelines, and standards and install and administer state data security systems on the state's computer facilities consistent with policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data.
Montana	Mont. Code § 2-6-1502	Each state agency that maintains personal information.	Develop procedures, as specified/detailed in statute, to protect personal information while enabling the state agency to use personal information as necessary for the performance of its duties under federal or state law.

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
Nevada	Nev. Rev. Stat. § 480.900 et seq.	State agencies; some provisions for local governments	Creates the Nevada Office of Cyber Defense Coordination to perform a variety of duties relating to the security of information systems of state agencies, including setting procedures for risk-based assessments; developing best practices for preparing for and mitigating such risks; preparing, maintaining and testing a statewide strategic plan regarding the security of information systems in Nevada. Requires the office to establish partnerships with local governments, the Nevada System of Higher Education and private entities. Requires each city or county to maintain a cybersecurity incident response plan.
New York	New York State Tech. Law § 103	State agencies.	Provides for the office of information technology services to advise and assist state agencies in developing policies, plans and programs for improving the statewide coordination, administration, security, confidentiality, program effectiveness, acquisition and deployment of technology. Also authorizes the office to

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			perform technology reviews and make recommendations for improving management and program effectiveness pertaining to technology; and to review and coordinate the purchase of technology by state agencies. Requires that, where applicable, the review should include but not be limited to: assessing consistency with the statewide strategic technology plan and agency technology plan; statewide technology standards; the safeguarding of information privacy; security of confidential records; and proper dissemination of public information. Also authorizes the office to o establish statewide technology policies, including but not limited to preferred technology standards and security, including statewide policies, standards, programs, and services relating to the security of state government nworks and geographic information systems. Also provides for the protection of the state government's cyber

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the state.
North Carolina	N.C. Gen. Stat. §143B-1376(a).	State agencies.	The state Chief Information Officer shall establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the state's distributed information technology assets, including communications and encryption technologies. The state CIO shall review and revise the security standards annually. As part of this function, the state Chief Information Officer shall review periodically existing security standards and practices in place among the various state agencies to determine whether those standards and practices meet statewide security and encryption requirements. The state Chief Information Officer may assume the direct

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			responsibility of providing for the information technology security of any State agency that fails to adhere to security standards adopted under this Article.
North Dakota	N.D. Century Code § 54-59-01 et seq.	State agencies, higher education institutions, counties, cities, school districts, or other political subdivisions.	Provides that the department of information technology shall advise and oversee cybersecurity strategy for the state agencies and institutions noted. Sets forth requirements for network services and requires the department to set proper measures for security, firewalls, and internet protocols addressing at the state's interface with other facilities.
Ohio	Ohio Rev. Code § 125.18	State agencies	Provides that the chief information officer shall establish policies and procedures for the security of personal information that is maintained and destroyed by state agencies. Provides for a chief information security officer (CISO) who is responsible for the implementation of such policies and procedures. Also provides for the CISO to assist agencies with IT security

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			strategic plans and to review those plans.
Oklahoma	62 Okl. St. § 34.32	Each state agency that has an information technology system.	Conduct an annual information security risk assessment to identify vulnerabilities associated with the information system. The final information security risk assessment report shall identify, prioritize, and document information security vulnerabilities for each of the state agencies assessed. Failure to comply with the requirements of this subsection may result in funding being withheld from the agency. State agencies shall use either the standard security risk assessment created by the Information Services Division or a third-party risk assessment meeting the ISO/IEC 17799 standards and using the National Institute of Standards and Technology Special Publication 800-30 (NIST SP800-30) process and approved by the Information Services Division.
Oregon	ORS § 182.122, 2016 Ore. Laws Chap. 110	State agencies	Provides for the Oregon Department of Administrative Services, in its sole discretion,

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			to (a) Review and verify the security of information systems operated by or on behalf of agencies; (b) Monitor state network traffic to identify and react to security threats; and (c) Conduct vulnerability assessments of agency information systems for the purpose of evaluating and responding to the susceptibility of information systems to attack, disruption or any other event that threatens the availability, integrity or confidentiality of information systems or the information stored in information systems.
South Carolina	2018-19 H.B. 4950 Act 264 (sec. 93.21) (appropriations)	All state agencies.	Adopt and implement cyber security policies, guidelines and standards developed by the Department of Administration. The department may conduct audits on state agencies as necessary to monitor compliance. Upon request, public institutions of higher learning, technical colleges, political subdivisions, and quasi-governmental bodies shall

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			submit sufficient evidence that their cyber security policies, guidelines and standards meet or exceed those adopted and implemented by the department. Exempts judicial and legislative branches.
Texas	Tex. Govt. Code § 2054.0286	State agencies	Provides for employment of a statewide data coordinator to improve the control and security of information collected by state agencies; Requires the statewide data coordinator to develop and implement best practices among state agencies to improve information management and analysis to increase information security.
Utah	Utah Code § 63F-2-102	State government	Creates a data security management council, which shall review existing state government data security policies, assess ongoing risks, notify state and local entities of new risks, coordinate breach simulation exercises, develop data security best practices recommendations for state government. Provides for hiring and training of a chief information

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			security officer for each government entity.
Vermont	56 Vt. Stat. § 3301 et seq.	State government	Authorizes the Agency of Digital Services to provide services for cybersecurity within state government and requires it to prepare a strategic plan about IT and cybersecurity to the General Assembly. Requires the agency to develop IT and cybersecurity policies and to conduct a security assessment for certain new IT projects.
Virginia	Va. Code § 2.2-603 Va. Code § 2.2-2009	Every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education	Every agency and department is responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the commonwealth's information technology security and risk-management program as set forth in § 2.2-2009, and shall report all known incidents that threaten data security. The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			government electronic information. Such policies, procedures, and standards will apply to the commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. The CIO shall also develop policies, procedures, and standards that address the scope of security audits and the frequency of such security audits. In addition, the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency
Washington	RCW 43.105.054 RCW 43.105.020, RCW § 43.105.215	State agencies (certain provisions also apply to institutions of higher education the legislature, and the judiciary)	Requires the Consolidated Technology Services Agency to establish security standards and policies to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure. Also provides for implementing a process for detecting, reporting, and responding to security

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			incidents. The director shall appoint a state chief information security officer. Requires each state agency, institution of higher education, the legislature, and the judiciary to develop an information technology security program that adheres to the office's security standards and policies. Requires each state agency to review and update its program annually and certify to the office that its program is in compliance with the office's security standards and policies. Requires state agencies to obtain an independent compliance audit at least once every three years.
West Virginia	W.V. Code § 5A-6-4a W.V. Code § 5A-6B-1 et seq.	Every agency and department.	The Chief Technology Officer is authorized to develop policies, procedures, standards and legislative rules that identify and require the adoption of practices to safeguard information systems, data and communications infrastructures. Provides for annual security audits of all executive branch agencies

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
			regarding the protection of government databases and data communications. Creates the West Virginia Cybersecurity Office under the supervision and control of a Chief Information Security Officer (CISO). Requires the CISO to develop policies, procedures and standards necessary to establish an enterprise cybersecurity program. Requires state agencies to undergo an appropriate cyber risk assessment; adhere to the cybersecurity standard established by the Chief Information Security Officer in the use of information technology infrastructure; and adhere to enterprise cybersecurity policies and standards. Also requires agencies to complete and submit a cyber risk self-assessment report and manage a plan of action and milestones based on the findings of the cyber risk assessment and business needs.

Data Security Laws--Government			
State	**Statutory Citation / Link**	**Applies to Government:**	**Statutory Summary/Excerpt**
Wyoming	Wyo. Stat. § 9-21-101	Every agency, department, board, commission, council, institution, separate operating agency or any other operating unit of the executive branch of state government.	Requires every agency to adopt, enforce and maintain a policy regarding the collection, access, security and use of data. The policy shall, at a minimum, comply with applicable federal and state law, adhere to standards set by the state chief information officer and include the following: (i) An inventory and description of all data required of, collected or stored by an agency; (ii) Authorization and authentication mechanisms for accessing the data; (iii) Administrative, physical and logical security safeguards, including employee training and data encryption; (iv) Privacy and security compliance standards; (v) Processes for identification of and response to data security incidents, including breach notification and mitigation procedures; (vi) In accordance with existing law, processes for the destruction and communication of data.

Source: National Conference of State Legislatures; nlcs.org

110 Cyber Security Facts from Varonis

Historical Data Brach Statistics

1. Worldwide spending on cybersecurity is forecasted to reach $133.7 billion in 2022. (Gartner)
2. 62% of businesses experienced phishing and social engineering attacks in 2018. (Cybint Solutions)
3. 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
4. Only 5% of companies' folders are properly protected, on average. (Varonis)
5. Data breaches exposed 4.1 billion records in the first half of 2019. (RiskBased)
6. 71% of breaches were financially motivated and 25% were motivated by espionage. (Verizon)
7. 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively. (Verizon)
8. Between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches. (ID Theft Resource Center)
9. While overall ransomware infections were down 52%, enterprise infections were up by 12% in 2018. (Symantec)
10. The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)
11. By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion. (Cybersecurity Media)

Largest Data Breaches and Hacking Statistics

12. Security breaches have increased by 11% since 2018 and 67% since 2014. (Accenture)
13. Hackers attack every 39 seconds, on average 2,244 times a day. (University of Maryland)
14. The average time to identify a breach in 2019 was 206 days. (IBM)
15. The average lifecycle of a breach was 314 days (from the breach to containment). (IBM)
16. 500 million consumers, dating back to 2014, had their information compromised in the Marriott-Starwood data breach made public in 2018. (Marriott)
17. 64% of Americans have never checked to see if they were affected by a data breach. (Varonis)
18. 56% of Americans don't know what steps to take in the event of a data breach. (Varonis)
19. The average cost of a data breach is $3.92 million as of 2019. (Security Intelligence)
20. 83% of enterprise workloads will move to the cloud by the year 2020. (Forbes)

21. In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time. (NY Times)
22. In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers. (Uber)
23. Uber tried to pay off hackers to delete the stolen data of 57 million users and keep the breach quiet. (Bloomberg)
24. In 2017, 412 million user accounts were stolen from Friendfinder's sites. (Wall Street Journal)
25. In 2017, 147.9 million consumers were affected by the Equifax Breach. (Equifax)
26. The Equifax breach cost the company over $4 billion in total. (Time Magazine)
27. In 2018, Under Armor reported that its "My Fitness Pal" was hacked, affecting 150 million users. (Under Armour)
28. 18 Russians, 19 Chinese individuals, 11 Iranians and one North Korean were involved in indictments for their alleged state-sponsored espionage against the United States. (Symantec)

Cyber Crime Statistics by Attack Type

29. 94% of malware was delivered by email. (Verizon)
30. Phishing levels declined, dropping from 1 in 2,995 emails in 2017, to 1 in 3,207 emails in 2018. (Symantec)
31. 34% of data breaches involved internal actors. (Verizon)
32. 51% of businesses experienced denial of service attacks in 2018. (Cybint Solutions)
33. 61% of organizations have experienced an IoT security incident. (CSO Online)
34. Malicious PowerShell scripts blocked in 2018 on the endpoint increased 1,000%. (Symantec)
35. 100,000 groups in at least 150 countries and more than 400,000 machines were infected by the Wannacry virus in 2017, at a total cost of around $4 billion. (Technology Inquirer)
36. IoT devices experience an average of 5,200 attacks per month. (Symantec)
37. 90% of remote code execution attacks are associated with cryptomining. (CSO Online)
38. The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)
39. 92% of malware is delivered by email. (CSO Online)
40. 48% of malicious email attachments are office files. (Symantec)
41. 69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus software.(Ponemon Institute's Cost of Data Breach Study)
42. Gandcab 5 requires that victims pay $2,499 for the decryption key. (McAfee)
43. 1 in 36 mobile devices had high risk apps installed. (Symantec)

44. In 2018, an average of 10,573 malicious mobile apps were blocked per day. (Symantec)
45. 65% of groups used spear-phishing as the primary infection vector. (Symantec)
46. Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16% of the attacks, was the third most common IoT threat in 2018. (Symantec)
47. 1 in 13 web requests lead to malware. (Symantec)
48. Ransomware detections have been more dominant in countries with higher numbers of internet-connected populations. The United States ranks highest with 18.2% of all ransomware attacks. (Symantec)
49. Most malicious domains, about 60%, are associated with spam campaigns. (Cisco)
50. About 20% of malicious domains are very new and used around 1 week after they are registered. (Cisco)

Cybersecurity Compliance and Governance Statistics

51. 69% of companies see compliance mandates driving spending. (CSO Online)
52. 53% of companies had over 1,000 sensitive files open to every employee. (Varonis)
53. 22% of all folders were available to every employee. (Varonis)
54. 88% companies spent more than $1 million on preparing for the GDPR. (CSO Online)
55. Google was fined $57 billion for GDPR violations by CNIL, a French data protection agency. (TechCrunch)
56. Companies reportedly spent $9 billion on preparing for the GDPR. (Forbes)
57. By December 2018, only 50% of companies believed they were GDPR compliant. (Data Center Frontier)
58. 15% of companies found 1,000,000+ files open to every employee. (Varonis)
59. 17% of all sensitive files were accessible to all employees. (Varonis)
60. On average, every employee had access to 17 million files. (Varonis)
61. The GDPR fines totaled $63 million in its first year. (GDPR.eu)
62. 1,000 news sources blocked EU readers to avoid the GDPR compliance rules. (Nieman Lab)
63. 61% of companies have over 500 accounts with non-expiring passwords. (Varonis)
64. Businesses spent $1.3 million on average to meet compliance requirements and are expected to put in an additional $1.8 million. (IAAP)
65. Legal advice and teams cost UK FTSE 350 companies about 40% of their GDPR budget or $2.4 million. (Forbes)
66. Since the GDPR was enacted, 31% of consumers feel their overall experience with companies has improved. (Marketing Week)
67. In the GDPR's first year, there were 144,000 complaints filed with various GDPR enforcement agencies and 89,000 data breaches recorded. (EDPB)

68. Equifax was found liable for their 2017 breach and was fined $425 million by the Federal Trade Commission (FTC) in 2019. (FTC)

Industry-Specific Cyber Stats

69. 43% of breach victims were small businesses. (Verizon)
70. Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%. (Varonis)
71. Financial services had 352,771 exposed sensitive files on average while Healthcare, Pharma and Biotech have 113,491 files on average — the highest when comparing industries. (Varonis)
72. 15% of breaches involved Healthcare organizations, 10% in the Financial industry and 16% in the Public Sector. (Verizon)
73. The banking industry incurred the most cybercrime costs in 2018 at $18.3 million (Accenture)
74. Smaller organizations (1–250 employees) have the highest targeted malicious email rate at 1 in 323. (Symantec)
75. WannaCry ransomware attack cost the National Health Service (NHS) over $100 million. (Datto)
76. The estimated losses in 2019 for the healthcare industry are $25 billion. (SafeAtLast)
77. Lifestyle (15%), and Entertainment (7%) were the most frequently seen categories of malicious apps. (Symantec)
78. Supply chain attacks are up 78% in 2019. (Symantec)
79. Trojan horse virus Ramnit largely affected the financial sector in 2017, accounting for 53% of attacks. (Cisco)
80. The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed. (Accenture)
81. The industry with the highest number of attacks by ransomware is the healthcare industry. Attacks will quadruple by 2020. (CSO Online)

Security Spending and Cost Statistics

82. By 2020, security services are expected to account for 50% of cybersecurity budgets. (Gartner)
83. The average cost of a malware attack on a company is $2.6 million. (Accenture)
84. **$**3.9 million is the average cost of a data breach. (IBM)
85. Healthcare had the highest data breach costs at $429 per record. (IBM)
86. The average cost per record stolen is $150. (IBM)
87. The total cost of cybercrime for each company increased by 12% from $11.7 million in 2017 to $13.0 million in 2018. (Accenture)
88. The average annual security spending per employee doubled, from $584 in 2012 to $1,178 in 2018. (Gartner)

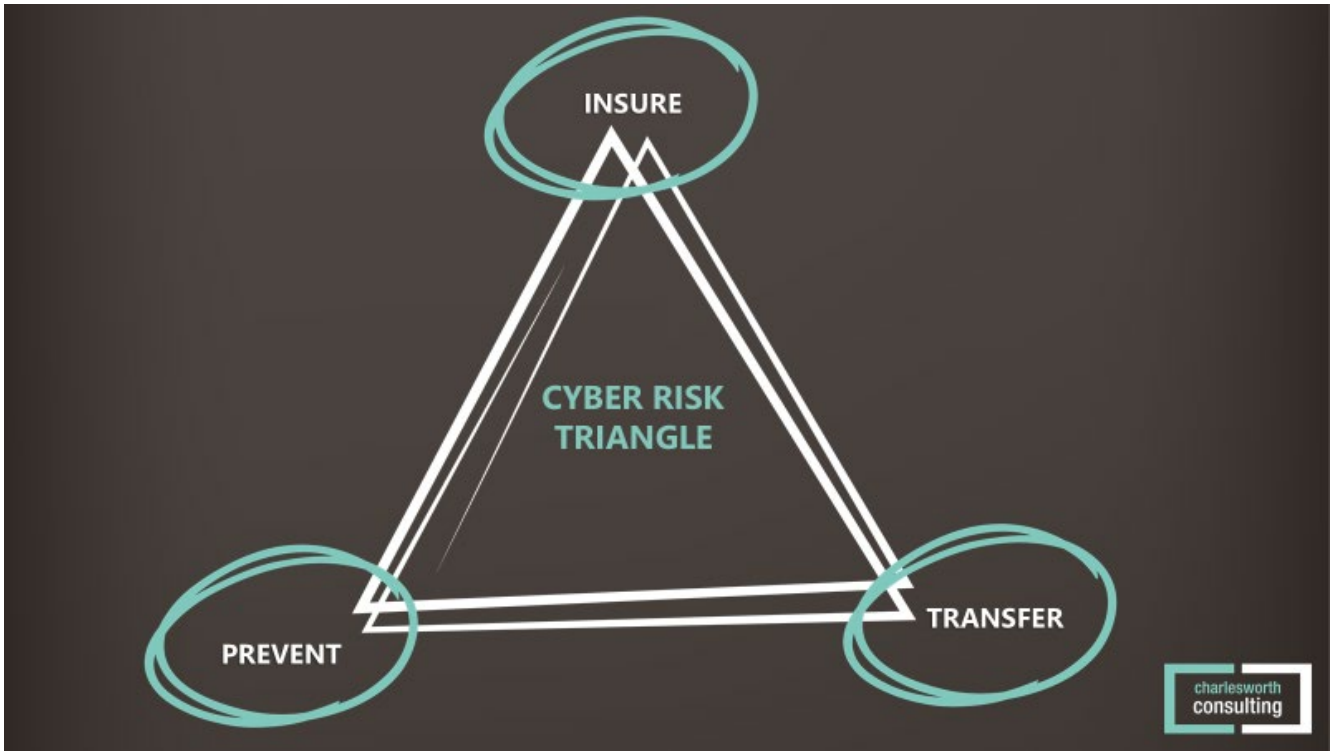
89. The cost of lost business averaged $1.42 million. (IBM)
90. The average cost in time of a malware attack is 50 days. (Accenture)
91. The most expensive component of a cyber attack is information loss at $5.9 million. (Accenture)
92. The average cost per lost or stolen records per individual is $141 — but that cost varies per country. Breaches are most expensive in the United States ($225) and Canada ($190). (Ponemon Institute's Cost of Data Breach Study)
93. In companies with over 50k compromised records, the average cost of a data breach is $6.3 million. (Ponemon Institute's Cost of Data Breach Study)
94. Including turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill, the cost of lost business globally was highest for U.S. companies at $4.13 million per company. (Ponemon Institute's Cost of Data Breach Study)
95. Damage related to cybercrime is projected to hit $6 trillion annually by 2021. (Cybersecurity Ventures)
96. Ransomware damage costs will rise to $11.5 billion in 2019 and a business will fall victim to a ransomware attack every 14 seconds at that time. (Cybersecurity Ventures)
97. The United States and the Middle East spend the most on post-data breach response. Costs in the U.S. were $1.56 million and $1.43 million in the Middle East. (Ponemon Institute's 2017 Cost of Data Breach Study)
98. 50% of large enterprises (with over 10,000 employees) are spending $1 million or more annually on security, with 43% spending $250,000 to $999,999, and just 7% spending under $250,000. (Cisco)

Cybersecurity Job Statistics

99. 82% of employers report a shortage of cybersecurity skills. (ISSA)
100. 61% of companies think their cybersecurity applicants aren't qualified. (ISSA)
101. The cybersecurity unemployment rate is 0% and is projected to remain there through 2021. (CSO Online)
102. It's predicted that by 2021, 100% of large companies globally will have a CISO position. (Cybersecurity Ventures)
103. By 2021, it's projected that there will be 3.5 million unfilled cybersecurity jobs globally. (Cybersecurity Ventures)
104. Information Security Analysts job positions in the US are expected to grow 32% from 2018–28. (Bureau of Labor Statistics)
105. Computer Network Architect job positions in the US are expected to grow 5% from 2018–28. (Bureau of Labor Statistics)

106. Computer Programmer job positions in the US are expected to decline 7% from 2018–28. (Bureau of Labor Statistics)
107. Since 2016, the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%, due to the GDPR demands. (Reuters)
108. 500,000 Data Protection Officers are employed (IAAP)
109. 66% of cybersecurity professionals struggle to define their career paths. (ISSA)
110. 60% of cybersecurity professionals aren't satisfied with their current job. (ISSA)

Effective Risk management isn't just about reducing liability exposure and buying insurance. You must look at the whole picture. **Manage cyber risks using the Cyber Risk Triangle**:



- **PREVENT**

Prevention is loss control for the digital world. The best way to reduce losses is to prevent them. Successful prevention includes a robust, well-funded IT department, a cyber security and mobile device policies, and a permission structure to protect PHI. Controlling exposure also includes training for employees. Remember, **30% of losses are caused by human error**, so your employees are one of your biggest vulnerabilities.

Meet with IT staff to understand what preventative steps are being taken to reduce the risk of loss. Review any relevant policies and provide feedback. Assess what resources are currently available to you, some of which you may not even be aware of.

- **TRANSFER**

Would you approve a road construction project if the contractor had no insurance and posted no bonds? The answer is obviously no, but many entities do this very thing when

contracting for IT services. IT vendors have entered nearly every governmental function. Most public entities use vendors for payment processing, utility billing, website hosting, software licensing, payroll, and human resources management. Law enforcement uses software to store police records and digital evidence, like photographs and videos. Yet many entities fail to take steps to transfer the risk of loss to the vendor. **City data is one of your most important assets**, and it should be treated as such.

Develop insurance requirements for IT contracts and implement controls to transfer risk from the City to the vendors. Oftentimes, cyber incidents are caused by vendors, not the City itself. Having contractual recourse and transferring the risk to the vendors can reduce the City's exposure.

- **INSURE**

Breaches happen, even with the best cyber security. And contracts get signed or can't be negotiated. This is where cyber liability insurance comes in. It fills all those gaps.

The cyber liability insurance market is evolving rapidly. New products are coming out every year, and carriers are constantly updating their policy forms to address new risks. Unlike property and casualty insurance policies, there is no "standard" form for cyber coverage. Polices can have different sublimits and exclusions, so it is important to review each policy form before making a decision. R**eview each policy form and identifying differences in coverage**.

sufficient to utilize the SaaS Services, you may unilaterally terminate this Agreement upon thirty (30) days written notice to us. You will not be entitled to a refund or offset of previously paid, but unused SaaS Fees.

2.5 Fees for Termination without Cause during Initial Term. If you terminate this Agreement during the initial term for any reason other than cause, Force Majeure, or lack of appropriations, or if we terminate this Agreement during the initial term for your failure to pay SaaS Fees, you shall pay us the following early termination fees:

a. if you terminate during the first year of the initial term, 100% of the SaaS Fees through the date of termination plus 25% of the SaaS Fees then due for the remainder of the initial term;

b. if you terminate during the second year of the initial term, 100% of the SaaS Fees through the date of termination plus 15% of the SaaS Fees then due for the remainder of the initial term; and

c. if you terminate after the second year of the initial term, 100% of the SaaS Fees through the date of termination plus 10% of the SaaS Fees then due for the remainder of the initial term.

SECTION G – INDEMNIFICATION, LIMITATION OF LIABILITY AND INSURANCE

1. Intellectual Property Infringement Indemnification.

1.1 We will defend you against any third party claim(s) that the [redacted] infringes that third party's patent, copyright, or trademark, or misappropriates its trade secrets, and will pay the amount of any resulting adverse final judgment (or settlement to which we consent). You must notify us promptly in writing of the claim and give us sole control over its defense or settlement. You agree to provide us with reasonable assistance, cooperation, and information in defending the claim at our expense.

1.2 Our obligations under this Section G(1) will not apply to the extent the claim or adverse final judgment is based on your use of the [redacted] in contradiction of this Agreement, including with non-licensed third parties, or your willful infringement.

1.3 If we receive information concerning an infringement or misappropriation claim related to the [redacted], we may, at our expense and without obligation to do so, either: (a) procure for you the right to continue its use; (b) modify it to make it non-infringing; or (c) replace it with a functional equivalent, in which case you will stop running the allegedly infringing [redacted] immediately. Alternatively, we may decide to litigate the claim to judgment, in which case you may continue to use the [redacted] consistent with the terms of this Agreement.

1.4 If an infringement or misappropriation claim is fully litigated and your use of the [redacted] is enjoined by a court of competent jurisdiction, in addition to paying any adverse final judgment (or settlement to which we consent), we will, at our option, either: (a) procure the right to continue its use; (b) modify it to make it non-infringing; or (c) replace it with a functional equivalent.

2. General Indemnification.

We will indemnify and hold harmless you and your agents, officials, and employees from and against any and all third-party claims, losses, liabilities, damages, costs, and expenses (including reasonable attorney's fees and costs) for (a) personal injury or property damage to the extent caused by our negligence or willful misconduct; or (b) our violation of PCI-DSS requirements or a law applicable to our performance under this Agreement. You must notify us promptly in writing of the claim and give us sole control over its defense or settlement. You agree to provide us with reasonable assistance, cooperation, and information in defending the claim at our expense.

2.1 To the extent permitted by applicable law, you will indemnify and hold harmless us and our agents, officials, and employees from and against any and all third-party claims, losses, liabilities, damages, costs, and expenses (including reasonable attorney's fees and costs) for personal injury or property damage to the extent caused by your negligence or willful misconduct; or (b) your violation of a law applicable to your performance under this Agreement. We will notify you promptly in writing of the claim and will give you sole control over its defense or settlement. We agree to provide you with reasonable assistance, cooperation, and information in defending the claim at your expense.

2.2 Notwithstanding anything to the contrary contained herein, [redacted] hereby acknowledges and agrees that Client's financial exposure for certain claims is limited by the Indiana Tort Claims Act, and Client's obligation to indemnify and save [redacted], its agents and employees harmless from and against any and all claims, damages, demands, penalties, costs, liabilities, losses, and expenses (including reasonable attorneys' fees and expenses at the trial and appellate levels) arising out of or related to claims subject to the Indiana Tort Claims Act shall be limited to the amount of damages available pursuant to Ind. Code § 34-13-3-4, as amended.

3. **DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN THIS AGREEMENT AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES, DUTIES, OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

4. **LIMITATION OF LIABILITY. EXCEPT AS OTHERWISE EXPRESSLY SET FORTH IN THIS AGREEMENT, OUR LIABILITY FOR DAMAGES ARISING OUT OF THIS AGREEMENT, WHETHER BASED ON A THEORY OF CONTRACT OR TORT, INCLUDING NEGLIGENCE AND STRICT LIABILITY, SHALL BE LIMITED TO YOUR ACTUAL DIRECT DAMAGES, NOT TO EXCEED (A) DURING THE INITIAL TERM, AS SET FORTH IN SECTION F(2), TOTAL FEES PAID AS OF THE TIME OF THE CLAIM; OR (B) DURING ANY RENEWAL TERM, THE THEN-CURRENT ANNUAL SAAS FEES PAYABLE IN THAT RENEWAL TERM. THE PARTIES ACKNOWLEDGE AND AGREE THAT THE PRICES SET FORTH IN THIS AGREEMENT ARE SET IN RELIANCE UPON THIS LIMITATION OF LIABILITY AND TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW, THE EXCLUSION OF CERTAIN DAMAGES, AND EACH SHALL APPLY REGARDLESS OF THE FAILURE OF AN ESSENTIAL PURPOSE OF ANY REMEDY. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO CLAIMS THAT ARE SUBJECT TO SECTIONS G(1) AND G(2).**

5. **EXCLUSION OF CERTAIN DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL WE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

6. Insurance. During the course of performing services under this Agreement, we agree to maintain

the following levels of insurance: (a) Commercial General Liability of at least $1,000,000; (b) Automobile Liability of at least $1,000,000; (c) Professional Liability of at least $1,000,000; (d) Workers Compensation complying with applicable statutory requirements; and (e) Excess/Umbrella Liability of at least $5,000,000. We will add you as an additional insured to our Commercial General Liability and Automobile Liability policies, which will automatically add you as an additional insured to our Excess/Umbrella Liability policy as well. We will provide you with copies of certificates of insurance upon your written request.

SECTION H – GENERAL TERMS AND CONDITIONS

1. Additional Products and Services. You may purchase additional products and services at the rates set forth in the Investment Summary for twelve (12) months from the Effective Date by executing a mutually agreed addendum. If no rate is provided in the Investment Summary, or those twelve (12) months have expired, you may purchase additional products and services at our then-current list price, also by executing a mutually agreed addendum. The terms of this Agreement will control any such additional purchase(s), unless otherwise specifically provided in the addendum.

2. Optional Items. Pricing for any listed optional products and services in the Investment Summary will be valid for twelve (12) months from the Effective Date.

3. Dispute Resolution. You agree to provide us with written notice within thirty (30) days of becoming aware of a dispute. You agree to cooperate with us in trying to reasonably resolve all disputes, including, if requested by either party, appointing a senior representative to meet and engage in good faith negotiations with our appointed senior representative. Senior representatives will convene within thirty (30) days of the written dispute notice, unless otherwise agreed. All meetings and discussions between senior representatives will be deemed confidential settlement discussions not subject to disclosure under Federal Rule of Evidence 408 or any similar applicable state rule. If we fail to resolve the dispute, either of us may assert our respective rights and remedies in a court of competent jurisdiction. Nothing in this section shall prevent you or us from seeking necessary injunctive relief during the dispute resolution procedures.

4. Taxes. The fees in the Investment Summary do not include any taxes, including, without limitation, sales, use, or excise tax. If you are a tax-exempt entity, you agree to provide us with a tax-exempt certificate. Otherwise, we will pay all applicable taxes to the proper authorities and you will reimburse us for such taxes. If you have a valid direct-pay permit, you agree to provide us with a copy. For clarity, we are responsible for paying our income taxes, both federal and state, as applicable, arising from our performance of this Agreement.

5. Nondiscrimination. We will not discriminate against any person employed or applying for employment concerning the performance of our responsibilities under this Agreement. This discrimination prohibition will apply to all matters of initial employment, tenure, and terms of employment, or otherwise with respect to any matter directly or indirectly relating to employment concerning race, color, religion, national origin, age, sex, sexual orientation, ancestry, disability that is unrelated to the individual's ability to perform the duties of a particular job or position, height, weight, marital status, or political affiliation. We will post, where appropriate, all notices related to nondiscrimination as may be required by applicable law.

6. E-Verify. We have complied, and will comply, with the E-Verify procedures administered by the U.S. Citizenship and Immigration Services Verification Division for all of our employees assigned to your

Cyber Insurance Requirements for Contracts

Example where data breach is primary concern:

Insurance: Vendor agrees to secure and maintain throughout the duration of this Agreement (with the exception of cyber liability insurance, all policies shall be on an occurrence basis unless otherwise agreed to), insurance of such types and in at least such amounts as required herein from an insurance company which carries a Best's Policyholder rating of "A" or better and carries at least a Class "VIII" financial rating, unless otherwise agreed to by the City. Vendor shall provide certificate(s) of insurance confirming the required protection on the standard Acord insurance certificate forms. Unless otherwise specified, City shall be shown as an additional insured on a primary and noncontributory basis on any applicable policies of insurance.

Cyber Liability Insurance

Policy must include: Privacy Liability, Privacy Regulatory Claims Coverage (where insurable by law), Security Breach Response Coverage, including notification expense, and Security Liability. Vendor shall maintain throughout the duration of this Agreement and for three (3) years thereafter.

Limits

Each type of coverage limit:	**$1,000,000 per occurrence**
Aggregate:	**$3,000,000**

Beware of Warranties

In addition to more detailed applications, many carriers are now requiring warranty statements by the applicant.

To Whom It May Concern:

The Applicant declares that no director, officer, employee or other proposed insured is aware of any acts, errors, omissions, circumstances or incidents or suspected incidents that reasonably might give rise to a claim or a privacy breach notification obligation under the proposed insurance.

(Must be signed by corporate officer with authority to sign on Applicant's behalf)

Warranties v. Representations

A representation is a statement made by the proposer to the insurer relating to a proposed risk. Such a representation may pertain to both material and immaterial facts. If material, then the representation must be substantially true. Any false statement on the material portion of the fact would render the contract voidable.

A warranty is an undertaking by the insured to the effect that he shall or shall not do a certain thing or that some conditions shall be fulfilled or whereby he affirms or negatives the existence of a particular state of affairs.

If the insurer wants to avoid the contract on grounds of misrepresentation, it must be proved that the misrepresentation relates to a material fact. With a warranty, any breach whether material or immaterial is enough for the insurer to void the contract.

Cyber Coverages

Cyber Incident Response – typical coverage may include first party coverage for incident response, legal fees, forensics, crisis communications, privacy breach assessments, and notification expenses

Cyber Crime – typical coverage may include first party coverage for losses resulting from cybercrimes, including fund transfer, extortion, and cyber ransom

System Damage and Business Interruption – typical coverage may include first party coverage for damage to hardware, including costs to recreate or rebuild network systems, device "bricking", and loss of income resulting from the loss

Network security and privacy liability – typical coverage may include third-party coverage against claims for how you handled personal information and network security, and regulatory fines

Media liability – typical coverage includes third party coverage against intellectual property claims as well as protection against libel, slander, and defamation