# Russia-Ukraine: Businesses assess cyber threat as U.S. moves to tighten cybersecurity

**SPECIAL REPORT | The Ukraine Crisis**

By Tony Foley, J.D.

*A review of recent federal cybersecurity actions; tips for assessing risk; and a list of state pre-breach security requirements*

As the Russian invasion of Ukraine continues, cybersecurity experts continue to raise the alarm concerning potential cyberattacks against Ukrainian targets as well as attacks against the U.S. and other NATO countries in response to the crippling sanctions imposed by those countries against Russia. More than three weeks into the conflict, the level of cyber intrusions has not risen to the level that experts had predicted, but the threat remains.

Spurred on by the increased threat level, Congress has moved to impose cyber incident notification requirements, and federal officials have emphasized the need for businesses to strengthen their cyber capabilities. Information on these responses, which have been in the works for some time but have taken on a new urgency in light of the war in Ukraine, are outlined below. Also, Appendix A lays out data security and information breach notification laws from all 50 states, and related tips on assessing cyber exposure risk from Greenberg Traurig's Jena Valdetero are included in Appendix B.

## CYBER INCIDENT REPORTING LEGISLATION IN OMNIBUS SPENDING BILL

On March 15, President Biden signed the Consolidated Appropriations Act of 2022. The spending bill includes language from the Cyber Incident Reporting for Critical Infrastructure Act (HR 5540), which is similar in many respects to legislation that cleared the Senate in early March as part of a package of cyber bills, the Strengthening American Cybersecurity Act (S 3600).

The cybersecurity provisions of the spending bill (see Division Y of the bill) create a Cyber Incident Review Office within the Cybersecurity and Infrastructure Security Agency (CISA) to receive confidential reports from critical infrastructure entities. Those entities will be required to report any cyber incident that the Homeland Security Secretary "determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States," according to the bill's text.

Payments to ransomware criminals would have to be reported within 24 hours. Compliance with the reporting obligations would be enforced through subpoenas and civil actions. Non-compliant entities would lose some of the liability protection they would otherwise obtain through compliance.

The law provides that the reporting requirements outlined above take effect on the dates prescribed in a final rule issued by CISA. Under the law's provisions, CISA has two years from the date of enactment to issue a notice of proposed rulemaking (NPRM) to promulgate rules to implement the requirements. Final rules must be issued within 18 months of the publication of the NPRM.

## SEC PROPOSES CYBER INCIDENT DISCLOSURE REQUIREMENTS

On March 9, the SEC announced proposed rules to enhance and standardize disclosure regarding cybersecurity risk management, strategy, governance and incident reporting. Specifically, the proposed rules, which are subject to a comment period of 60 days from the date of the announcement or 30 days after the publication of the proposed rules in the *Federal Register,* would:

- Require current reporting about material cybersecurity incidents on Form 8-K; and
- Require periodic disclosures regarding, among other things:
  - A registrant's policies and procedures to identify and manage cybersecurity risks;
  - Management's role in implementing cybersecurity policies and procedures;
  - Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - Updates about previously reported material cybersecurity incidents.

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

## INTELLIGENCE OFFICIALS WARN OF "SPILLOVER" CYBER ATTACKS

Speaking to the House Intelligence Committee on March 8, intelligence officials said that while the U.S. and its allies have not yet experienced significant cyberattacks in relation to the war in Ukraine, such attacks may still yet come. FBI Director Christopher Wray reminded the committee of the NotPetya cyberattack in 2017, which was launched from Russia and designed to concentrate on Ukraine, but the malware used in the attack spread to other, unintended targets.

"[E]ven if the Russians think they have carefully calibrated some form of malicious cyber activity against critical infrastructure, the reality is they've shown a history of not being able to manage the effects of it as well as they intend," Mr. Wray said. "NotPetya is widely viewed as one of the most destructive attacks in history. That's a GRU [Russian military intelligence] attack that had that kind of spillover effect. That's something we're deeply concerned about."

Paul Nakasone, Director of the National Security Agency and Commander of U.S. Cyber Command, expressed similar concerns. "We're very very focused on some type of cyber activity that's designed for Ukraine that spreads more broadly into other countries," he told the committee.

The testimony was given during the committee's annual worldwide threats hearing, which, while focused on the threat of nuclear weapons and other kinetic attacks related to the invasion of Ukraine, also offered warnings of offensive cyberattacks. The government's annual threat assessment, which was discussed at the hearing, identified China as the primary threat actor in cyber espionage but emphasized that the Russian threat remains prominent. "Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. We assess that Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions, as well as a deterrence and military tool," the assessment said. "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."

## CISA URGES DILIGENCE, LAUNCHES "SHIELDS UP" PAGE

Originally launched in February as a response to the then impending invasion, the "Shields Up" page initiated by CISA notes that Russian cyberattacks against Ukraine's government and critical infrastructure organizations may also impact organizations beyond the region. The Shields Up page provides access to the latest updates on vulnerabilities that have been exploited by Russian cyber threat actors, and offers recommended actions to be taken by all organizations, regardless of size, in adopting a heightened posture regarding cybersecurity. These recommendations include the following:

- Steps to reduce the risk of a damaging cyber intrusion, including ensuring that all software updates are in place, particularly with respect to known vulnerabilities;
- Steps to quickly detect a potential intrusion, including ensuring that IT personnel are focused on identifying and quickly assessing unexpected or unusual network behavior;
- Ensuring that an organization is prepared to respond to an intrusion, including by designating a crisis response team and assuring the availability of key personnel; and
- Maximizing an organization's resilience to a cyber incident, including implementing and testing backup procedures to ensure that critical data can be restored if the organization is impacted by ransomware or a destructive cyberattack.

The Shields Up page provides further guidance specific to corporate leaders and information on responses to ransomware attacks (including a Ransomware Guide that includes a checklist organizations can use to guide themselves through the response process).

> "Every organization—large and small—must be prepared to respond to disruptive cyber activity," CISA said. "As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyber-attacks. When cyber incidents are reported quickly, we can use this information to render assistance and as a warning to prevent other organizations and entities from falling victim to a similar attack."

## DHS TAKES LEAD IN RESPONSE TO RUSSIAN THREATS

On February 24, President Biden named the Department of Homeland Security (DHS) as the lead federal agency to coordinate domestic preparedness and response efforts related to the Russia-Ukraine crisis. In a press release acknowledging this role,

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

DHS said that it has established a Unified Coordination Group (UCG) to ensure unity of effort across the federal government in preparing for and responding to possible threats to the homeland; development and pursuit of strategic objectives and priorities; and coordination with federal, state, local, tribal, and territorial officials, as well as representatives of the private sector and nongovernmental entities in support of these objectives and priorities.

DHS encourages all organizations to improve both their physical and cyber resilience and recommends that organizations consult the CISA Shields Up page for information on improving their cybersecurity and protecting their critical assets.

## BREACH NOTIFICATION AND CYBER INSURANCE LIKELY TO BE MAJOR ISSUES

As the situation in Ukraine evolves, together with the potential for Russian cyberattacks, the odds of a data breach or other cyber event are likely to increase. In Appendix A we list pre-breach security measures that are required of businesses by the states, as taken from the Breach Notification Jurisdictional Compare Smart Chart, available on the Cybersecurity & Privacy dashboard on Wolters Kluwer's ***VitalLaw*** research platform.

Additionally, the increased risk of cyberattacks makes now a good time for businesses to evaluate their cyber insurance needs and to reassess their current coverages. Jena Valdetero, Co-Chair of the U.S. Data, Privacy and Cybersecurity Practice at Greenberg Traurig and the author of the Smart Task on Evaluating Cyber Liability Insurance, also available on the Cybersecurity & Privacy dashboard on ***VitalLaw***, makes several recommendations. These include determining the level of insurance coverage a business requires, conducting a cyber exposure risk assessment that measures the business' cybersecurity program against recognized industry best practices and regulatory requirements, reviewing third party vendor security exposure, and identifying known threats, among other suggestions. A helpful assessment checklist from Ms. Valdetero's Smart Task is available in Appendix B below. ■

## APPENDIX A – PRE-BREACH SECURITY MEASURES

**Source:** Breach Notification Jurisdictional Compare Smart Chart, *WK VitalLaw* (available to subscribers of the VitalLaw Cybersecurity and Privacy Law Suite).

In some cases, businesses are required to take measures to safeguard data containing customers' personal information in their possession

| Jurisdiction | Answer | Citation |
|---|---|---|
| Federal | Entities subject to the HIPAA Security Rule must adhere to the rule's requirements regarding the protection of electronic personal health information created, used or maintained by the entity. | 45 CFR Sec. 164.302, et seq. ; 45 CFR Sec. 164.500, et seq. |
| Alabama | Covered entities and third-party agents must implement and maintain reasonable security measures, including, as practicable, designation of an employee or employees to coordinate security measures; identification of internal and external risks of a breach of security; and adoption of appropriate information safeguards. | Alabama Code Sec. 8-38-3 |
| Alaska | State law does not provide for security measures generally applicable to businesses. | Alaska Statutes Sec. 45.48.010 through 45.48.995 |
| Arizona | State law does not provide for security measures generally applicable to businesses. | Arizona Revised Statutes Sec. 18-551 through 18-552 |
| Arkansas | Entities must implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure. | Arkansas Code Sec. 4-110-104(b) |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

**APPENDIX A – PRE-BREACH SECURITY MEASURES** *Continued*

| Jurisdiction | Answer | Citation |
|---|---|---|
| California | Businesses owning or licensing personal information about California residents must implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. | California Civil Code Sec. 1798.81.5(b) |
| Colorado | Covered entities that maintain, own, or license personal identifying information about state residents must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations. Similar provisions apply to government entities. | Colorado Revised Statutes Sec. 6-1-713.5; Colorado Revised Statutes Sec. 24-73-103(2)(a) |
| Connecticut | A person in possession of personal information of another person must safeguard the data, computer files and documents containing the information from misuse by third parties. In addition, a person who collects social security numbers must create a privacy protection policy to protect the confidentiality of, prohibit unlawful disclosure of, and limit access to such numbers. | Connecticut General Statutes Sec. 42-471 |
| Delaware | Any person who conducts business in the state and owns, licenses or maintains personal information must implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure or destruction of personal information collected or maintained in the regular course of business. | Delaware Code Annotated Title 6, Sec. 12B-100 |
| District of Columbia | Persons or entities that own, license or otherwise possess personal information of residents must implement and maintain reasonable security safeguards, including procedures and practices appropriate to the nature and size of the entity or operation. Persons or entities using a nonaffiliated third party as a service provider and that discloses personal information to that party must have a written agreement with the party requiring it to maintain the same security measures. Persons or entities subject to security requirements under the Gramm Leach Bliley Act, HIPAA Privacy Rule or HITECH requirements are deemed to be in compliance with district requirements. | District of Columbia Code Sec. 28-3852(a) |
| Florida | Covered entities, governmental entities and third-party agents must take reasonable measures to protect and secure data in electronic form containing personal information. | Florida Statutes Sec. 501.171(2) |
| Georgia | State law does not provide for security measures generally applicable to businesses. | Georgia Code Annotated Title 10, Chapter 1, Article 34, Sec. 10-1-910 through 10-1-912 |
| Hawaii | State breach notification law does not provide for security measures generally applicable to businesses. Effective July 1, 2021, insurance licensees must develop, implement and maintain a comprehensive written information security program containing administrative, technical and physical safeguards for the protection of personal information and the licensee's information system. Licensees generally have until July 1, 2022, to implement the program, and have until July 1, 2023, to impose specified security requirements on third-party service providers. | Hawaii Revised Statutes Sec. 487N-1 through 487N-4; SB 1100, Laws 2021, to be codified in Haw. Rev. Stat. as a new article of Title 24, Chapter 431 (see Part II of bill) |
| Idaho | State law does not provide for security measures generally applicable to businesses. | Idaho Code Sec. 28-51-104 through 28-51-107 |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

**APPENDIX A – PRE-BREACH SECURITY MEASURES** *Continued*

| Jurisdiction | Answer | Citation |
|---|---|---|
| Illinois | A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. | 815 Illinois Compiled Statutes Sec. 530.45 |
| Indiana | Database owners must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect personal information of Indiana residents. Effective July 1, 2021, insurance licensees are subject to specific provisions regarding the development of an information security program meeting statutory requirements. | Indiana Code Sec. 24-4.9-3-3.5(c); Indiana Code Sec. 27-2-27-16 through 27-2-27-20 |
| Iowa | State law does not provide for security measures generally applicable to businesses. Effective January 1, 2022, specified licensed insurers are subject to requirements regarding the implementation of an information security program and cybersecurity investigation and notification requirements (Iowa Code Sec. 507F.1, et seq., as added by H.F. 719, Laws 2021). | Iowa Code Sec. 715C.1 through 715C.2 |
| Kansas | Holders of personal information must implement and maintain reasonable procedures and practices appropriate to the nature of the information and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. A holder that complies with federal or state laws or regulations regarding data security are deemed to be in compliance with this requirement. | Kansas Statutes Sec. 50-6,139b |
| Kentucky | State law does not provide for security measures generally applicable to businesses. | Kentucky Revised Statutes Sec. 365.732 |
| Louisiana | Under the state's data breach notification law, any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Under the Insurance Data Security Law, effective 8/1/2021, licensees are required to develop, implement and maintain a comprehensive, written information security program meeting a variety of statutory criteria. Effective 8/1/2022, if the licensee uses a third-party service provider to maintain, process or store its nonpublic information, the licensee must require the provider to implement an equivalent program. | Louisiana Revised Statutes, Title 51, Sec. 3074(A) Louisiana Revised Statutes Title 22, Sec. 2504 |
| Maine | State law does not provide for security measures generally applicable to businesses. Effective January 1, 2022, specified licensed insurers are subject to requirements regarding the implementation of an information security program and cybersecurity investigation and notification requirements (Maine Revised Statutes, Title 24-A, Sec. 2261, et seq., as added by L.D. 51, Laws 2021). | Maine Revised Statutes, Title 10, Sec. 1346 through 1350-A |
| Maryland | Businesses must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations to protect the information from unauthorized access, use, modification or disclosure. | Maryland Annotated Code, Commercial, Sec. 14-3503 |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

**APPENDIX A – PRE-BREACH SECURITY MEASURES** *Continued*

| Jurisdiction | Answer | Citation |
|---|---|---|
| Massachusetts | The Department of Consumer Affairs and Business Regulation has adopted data security regulations relative to owners of personal data to safeguard such data. Persons who own, license, store or maintain personal information about a resident must develop and implement a comprehensive information security program containing administrative, technical and physical safeguards appropriate to the size of the business, the resources available, the amount of stored data, and the need for security and confidentiality of consumer and employee information. The regulations also contain specific computer security requirements. | Massachusetts Regulations, 201 CMR 17.00, Sec. 17.01 through 17.05 |
| Michigan | State law does not provide for security measures generally applicable to businesses. | Michigan Compiled Laws Sec. 445.61 through 445.73 |
| Minnesota | State breach notification law does not provide for security measures generally applicable to businesses. Portal operators and MNvest issuers must take reasonable steps to ensure that a purchaser's financial and personal information is properly secured, as specified by regulation. Effective August 1, 2021, licensees must develop, implement and maintain a comprehensive written information security program containing administrative, technical and physical safeguards for the protection of personal information and the licensee's information system. Licensees generally have until August 1, 2022, to implement the program, and have until August 1, 2023, to impose specified security requirements on third-party service providers. | Minnesota Statutes Sec. 325E.61; Minn. Admin. Rules 2876.3055(1)(A); Minn. Stat. Sec. 60A.9851, as added by Ch. 4 (HF 6), Laws 2021, First Extraordinary Session, Sec. 6 |
| Mississippi | State law does not provide for security measures generally applicable to businesses. | Mississippi Code Sec. 75-24-29 |
| Missouri | State law does not provide for security measures generally applicable to businesses. | Missouri Revised Statutes Sec. 407.1500 |
| Montana | State law does not provide for security measures generally applicable to businesses. | Montana Code Sec. 30-14-1701 through 30-14-1705 and Sec. 33-19-321 |
| Nebraska | An individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident must implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, to protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information. | Nebraska Revised Statutes Sec. 87-808(1) |
| Nevada | A data collector that maintains records which contain personal information of a resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. | Nevada Revised Statutes Sec. 603A.210 |
| New Hampshire | State law does not provide for security measures generally applicable to businesses. | New Hampshire Revised Statutes Sec. 359-C:19 through 359-C:21 |
| New Jersey | State law does not provide for security measures generally applicable to businesses. | New Jersey Statutes Annotated, Sec. 56:8-161 through 56:8-165 |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

**APPENDIX A – PRE-BREACH SECURITY MEASURES** *Continued*

| Jurisdiction | Answer | Citation |
|---|---|---|
| New Mexico | A person that owns or licenses personal identifying information of a resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure. | New Mexico Statutes Sec. 57-12-4 |
| New York | State law does not provide for security measures generally applicable to businesses. However, New York regulations do impose cybersecurity requirements applicable to banks, financial service companies and insurers, as well as credit reporting agencies. | 23 New York Codes, Rules and Regulations, Sec. 500.0 through 500.23; 23 New York Codes, Rules and Regulations, Sec. 201.07 |
| North Carolina | State law does not provide for security measures generally applicable to businesses. | North Carolina General Statutes Sec. 75-60 through 75-65 |
| North Dakota | State law does not provide for security measures generally applicable to businesses. Effective August 1, 2022, specified licensed insurers are subject to requirements regarding the implementation of an information security program and cybersecurity investigation and notification requirements (North Dakota Century Code Sec. 26.1-02.2-01, et seq., as added by S.B. 2075, Laws 2021). | North Dakota Century Code Sec. 51-30-01 through 51-30-07 |
| Ohio | Covered entities seeking to insulate themselves from liability related to the failure to implement reasonable information security controls resulting in a data breach must create, maintain and comply with a written cybersecurity program meeting statutory requirements, including protecting against anticipated threats to the security and integrity of the information and unauthorized access to the information likely to result in identity theft. | Ohio Revised Code Sec. 1354.01 through 1354.05 |
| Oklahoma | State law does not provide for security measures generally applicable to businesses. | Oklahoma Statutes, Title 24, Sec. 161 |
| Oregon | Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data. | Oregon Revised Statutes Sec. 646A.622(1) |
| Pennsylvania | State law does not provide for security measures generally applicable to businesses. | Pennsylvania Consolidated Statutes, Title 73, Sec. 2301 through 2329 |
| Rhode Island | A business that stores, collects, processes, maintains, acquires, uses, owns, or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based security program in order to protect against unauthorized access, destruction, use, modification, or disclosure. | Rhode Island General Laws Sec. 11-49.3-2(a) |
| South Carolina | State law does not provide for security measures generally applicable to businesses. | South Carolina Code Sec. 39-1-90 |
| South Dakota | State law does not provide for security measures generally applicable to businesses. | South Dakota Code Laws Sec. 22-40-19 through 22-40-26 |
| Tennessee | The breach notification law does not provide for security measures generally applicable to businesses.<br><br>Provisions requiring covered insurers to implement an information security program and to investigate and notify cybersecurity events provide that covered licensees must implement such a program by July 1, 2022. The law provides for the elements of the program. | Tennessee Code Annotated Sec. 47-18-2107; Tennessee Code Annotated Sec. 56-2-1004 |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

**APPENDIX A – PRE-BREACH SECURITY MEASURES** *Continued*

| Jurisdiction | Answer | Citation |
|---|---|---|
| Texas | A business must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. | Texas Business and Commerce Code Title 11, Subtitle B, Chapter 521, Sec. 521.052(a) |
| Utah | Any person who conducts business in the state and maintains personal information must implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business. | Utah Code Sec. 13-44-201(1)(a) |
| Vermont | State law does not provide for security measures generally applicable to businesses. Effective January 1, 2019, specific provisions require data brokers to develop, implement and maintain a comprehensive information security program containing administrative, technical and physical safeguards appropriate to the size, scope and type of business of the broker, resources available to the broker, the amount of stored data and the need for security and confidentiality of personally identifiable information. The law also includes requirements regarding computer system security. | Vermont Statutes, Title 9, Sec. 2447 |
| Virginia | State law does not provide for security measures generally applicable to businesses. | Virginia Code Sec. 18.2-186.6 |
| Washington | State law does not provide for security measures generally applicable to businesses. A person that knowingly possesses a biometric identifier that has been enrolled for a commercial purpose must take reasonable care to guard against unauthorized access to and acquisition of such identifiers. | Washington Revised Code Sec. 19.255.010; Washington Revised Code Sec. 19.375.020(4)(a) |
| West Virginia | State law does not provide for security measures generally applicable to businesses. | West Virginia Code Sec. 46A-2A-101 through 46A-2A-105 |
| Wisconsin | State breach notification law does not provide for security measures generally applicable to businesses. Effective November 1, 2021, insurance licensees must develop, implement and maintain a comprehensive written information security program containing administrative, technical and physical safeguards for the protection of personal information and the licensee's information system. Licensees generally have until November 1, 2022, to implement the program, and have until November 1, 2023, to impose specified security requirements on third-party service providers. These requirements do not apply to specified small insurers. | Wisconsin Statutes Sec. 134.98 |
| Wyoming | State law does not provide for security measures generally applicable to businesses. | Wyoming Statutes Sec. 40-12-501 through 40-12-509 |

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

## APPENDIX B – ASSESSING CYBER EXPOSURE RISK

**Source:** WK Smart Task, *Evaluating Cyber Liability Insurance*
by Jena Valdetero, Co-Chair, U.S. Data, Privacy and Cybersecurity Practice at Greenberg Traurig

### Assess cyber exposure risk

A tool that may help the organization assess its cyber exposure risk is a cyber exposure risk assessment:

Assessment checklist:

- Assess the organization's cyber¬ security program against industry best practices such as the frameworks created by the National Institute of Standards and Technology (NIST), the SANS Institute's CIS Critical Security Controls, or the International Standards Organization (ISO) 27001;
- Evaluate the organization's data-breach response plan against the regulatory requirements implicated by the business' operations (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc.).
- Review third-party vendors and suppliers' security exposures and their ability to access your network and data;
- Review privacy protocols and records databases (including assessing the information are you collecting and storing, why you are collecting and storing it);
- Identify any cyber risks your company has assumed in contracts with other service providers;
- Identify any known threats (e.g., ransomware, phishing attempts including "spear-phishing" and software vulnerabilities);
- Review employee training programs; and
- Approximate the potential causal effects of a cyber incident to the organization such as bodily injury or property damage due to disruption of operational technology (as opposed to information technology), supply chain disruption, loss of intellectual property, and reputational impact.

***Practitioner's Tip*** – If the organization does not have the internal expertise to conduct this assessment, there are a plethora of reputable legal and consultancy practices that specialize in these types of reviews for organizations of all types. Retaining experts will ensure that you're assessing against the most up-to-date industry best-practices and legal requirements. Also, it is important that the assessment should involve stakeholders from all areas of the organization: privacy, information security, risk management, legal, information technology, business operations, etc. Cyber risk is not unique to the information technology department. Cyber risks can arise in all areas of the company, so all must be assessed.

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.