HINSHAW

News

Annmarie Giblin Discusses in National Media Outlets Heightened Cybersecurity Risks Amid Ukraine Conflict

March 7, 2022

Hinshaw attorney Annmarie Giblin was quoted extensively in several national media outlets regarding the cybersecurity risks to U.S. businesses in light of the Ukraine conflict.

She discussed specific threat vectors, recommended a series of cyberrisk management steps, and analyzed the impact on cyber insurance.

Business Journals: One pressing small-business concern amid Ukraine conflict? Cybersecurity issues

Read the full *Business Journals* article (*subscription may be required*)

Giblin, said experts are seeing troubling new types of malware being deployed against Ukraine's government and its banking system: "It is only a matter of time before we start seeing these threats employed against U.S. businesses.".

She added that small and midsize businesses without the resources of larger companies could be vulnerable.

The traditional industry focus on larger companies, who have the resources to have a much more secure cybersecurity posture than small to midsized businesses, has been misplaced, because the small to midsized businesses are the vendors, customers and business partners of the larger companies and our government, and they remain an incredibly soft target.

Regardless of size, Giblin said businesses would be wise to dust off their cybersecurity incident response plans and take a critical look at whether they are sufficient to respond to new types of malware.

One of the more troubling ones we are seeing in Ukraine is this data-wiping malware, HermeticWiper, which is just starting to be deployed but seems to have been installed on computers months beforehand. Businesses should have their security teams gathering research about this strain, looking for this malware on their systems, but also ensure they have the proper backups of the business' data and that those backups are secure and housed separate and apart from their main system.

Service Areas

Privacy, Security & Artificial Intelligence

Offices

New York

Cybersecurity Dive: Ukraine war tests cyber insurance exclusions

Read the full *Cybersecurity* Dive article

"Regardless of the crisis in Ukraine, companies of all sizes will likely be seeing higher premiums and stricter underwriting this renewal season," said Giblin.

The changes were not only related to higher cybersecurity risks due to COVID-19, the Ukraine conflict and other risk factors, she added. There are also changing "reasonableness" standards of what an effective cybersecurity risk management program should include.

Risk Management Monitor: Cyberrisk Management Tips for Businesses Amid the Russia-Ukraine War

Read the full *Risk Management Monitor* article

“In addition to taking a fresh look at plans and other policies within an organization’s cybersecurity risk framework, businesses should consider a few common-sense tips to prepare for a potential cyber incident,” advised Giblin. She recommended risk professionals take the following steps to boost cyberrisk management efforts right now:

1. Print out a hard copy of any necessary polices and plans, like the cyber incident response plan, the business’ cyber insurance policy and a contact list for the organization, so you have them available in the event you cannot access your system and need to communicate with employees through alternative methods.
2. Remind your employees about common cyber scams and reiterate that there will be no retaliation for reporting a cybersecurity mistake, such as clicking on a bad link.
3. Have key members of the executive team and incident response team set up a secure but alternate method of communication, such as sharing phone numbers or creating a different off system email address to communicate in the event the business’ systems are not available or not trusted.
4. Keep track of the latest threats and get the research over to your IT team so they can update your firewall, and/or contact the business’ security services provider and make sure they are aware of and addressing these new malware strains.
5. Evaluate and if possible, test your business continuity plans. Organizations should be asking themselves, “What does the work day look like without access to the business’ systems?” and “How can we still work without any technology support?”

"One pressing small-business concern amid Ukraine conflict? Cybersecurity issues" was distributed by *Business Journals*, February 28, 2022

"Ukraine war tests cyber insurance exclusions" was published by *Cybersecurity Dive*, March 3, 2022

"Cyberrisk Management Tips for Businesses Amid the Russia-Ukraine War" was published by *Risk Management Monitor*, March 4, 2022