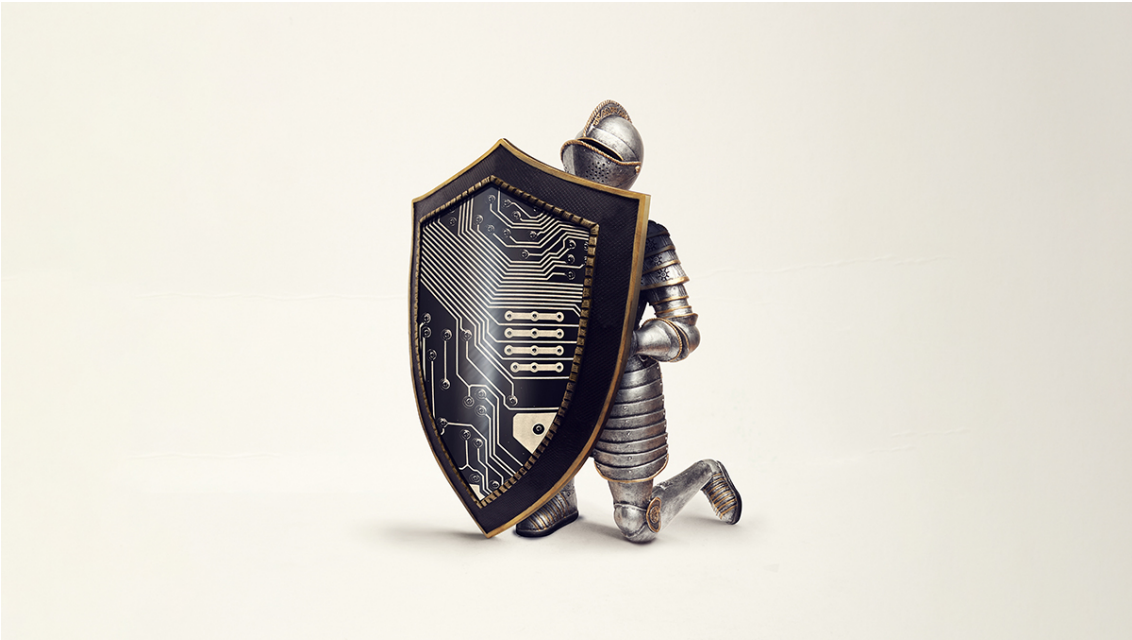
Harvard
Business
Review

Cybersecurity And Digital Privacy

New Cybersecurity Regulations Are Coming. Here's How to Prepare.

by Stuart Madnick

August 29, 2022



C. J. Burton/Getty Images

Summary. A whole suite of new cybersecurity regulations and enforcement are in the offing, both at the state and federal level in the U.S. and around the world. Companies don't need to just sit by and wait for the rules to be written and then implemented, however. Rather, they need to be working now to understand the kinds of regulations that are presently being considered, ascertain the uncertainties and potential impacts, and prepare to act. **close**

Cybersecurity has reached a tipping point. After decades of private-sector organizations more or less being left to deal with cyber incidents on their own, the scale and impact of cyberattacks means that the fallout from these incidents can ripple across societies and borders.

Now, governments feel a need to "do something," and many are considering new laws and regulations. Yet lawmakers often struggle to regulate technology — they respond to political urgency, and most don't have a firm grasp on the technology they're aiming to control. The consequences, impacts, and uncertainties on companies are often not realized until afterward.

In the United States, a whole suite of new regulations and enforcement are in the offing: the Federal Trade Commission, Food and Drug Administration, Department of Transportation, Department of Energy, and Cybersecurity and Infrastructure Security Agency are all working on new rules. In addition, in 2021 alone, 36 states enacted new cybersecurity legislation. Globally, there are many initiatives such as China and Russia's data localization requirements, India's CERT-In incident reporting requirements, and the EU's GDPR and its incident reporting.

Companies don't need to just sit by and wait for the rules to be written and then implemented, however. Rather, they need to be working now to understand the kinds of regulations that are presently being considered, ascertain the uncertainties and potential impacts, and prepare to act.

What We Don't Know About Cyberattacks

To date, most countries' cybersecurity-related regulations have been focused on privacy rather than cybersecurity, thus most cybersecurity attacks are not required to be reported. If private information is stolen, such as names and credit card numbers, that must be reported to the appropriate authority. But, for instance, when Colonial Pipeline suffered a ransomware attack that caused it to shut down the pipeline that provided fuel to

nearly 50% of the U.S. east coast, it wasn't required to report it because no personal information was stolen. (Of course, it is hard to keep things secret when thousands of gasoline stations can't get fuel.)

As a result, it's almost impossible to know how many cyberattacks there really are, and what form they take. Some have suggested that only 25% of cybersecurity incidents are reported, others say only about 18%, others say that 10% or less are reported.

The truth is that we don't know what we don't know. This is a terrible situation. As the management guru Peter Drucker famously said: "If you can't measure it, you can't manage it."

What Needs To Be Reported, by Whom, and When?

Governments have decided that this approach is untenable. In the United States, for instance, the White House, Congress, the Securities and Exchange Commission (SEC), and many other agencies and local governments are considering, pursuing, or starting to enforce new rules that would require companies to report cyber incidents — especially critical infrastructure industries, such as energy, health care, communications and financial services. Under these new rules, Colonial Pipeline would be required to report a ransomware attack.

To an extent, these requirements have been inspired by the reporting recommended for "near misses" or "close calls" for aircraft: When aircraft come close to crashing, they're required to file a report, so that failures that cause such events can be identified and avoided in the future.

On its face, a similar requirement for cybersecurity seems very reasonable. The problem is, what should count as a cybersecurity "incident" is much less clear than the "near miss" of two aircraft being closer than allowed. A cyber "incident" is something that could have led to a cyber breach, but does not need to have

become an actual cyber breach: By one official definition, it only requires an action that "imminently jeopardizes" a system or presents an "imminent threat" of violating a law.

This leaves companies navigating a lot of gray area, however. For example, if someone tries to log in to your system but is denied because the password is wrong. Is that an "imminent threat"? What about a phishing email? Or someone searching for a known, common vulnerability, such as the log4j vulnerability, in your system? What if an attacker actually got into your system, but was discovered and expelled before any harm had been done?

This ambiguity requires companies and regulators to strike a balance. All companies are safer when there's more information about what attackers are trying to do, but that requires companies to report meaningful incidents in a timely manner. For example, based on data gathered from current incident reports, we learned that just 288 out of the nearly 200,000 known vulnerabilities in the National Vulnerability Database (NVD) are actively being exploited in ransomware attacks. Knowing this allows companies to prioritize addressing these vulnerabilities.

On the other hand, using an overly broad definition might mean that a typical large company might be required to report thousands of incidents per day, even if most were spam emails that were ignored or repelled. This would be an enormous burden both on the company to produce these reports as well as the agency that would need to process and make sense out of such a deluge of reports.

International companies will also need to navigate the different reporting standards in the European Union, Australia, and elsewhere, including how quickly a report must be filed — whether that's six hours in India, 72 hours in the EU under GDPR, or four business days in the Unites States, and often many variations in each country since there is a flood of regulations coming out of diverse agencies.

What Companies Can Do Now

Make sure your procedures are up to the task.

Companies subject to SEC regulations, which includes most large companies in the United States, need to quickly define "materiality" and review their current policies and procedures for determining whether "materiality" applies, in light of these new regulations. They'll likely need to revise them to streamline their operation — especially if such decisions must be done frequently and quickly.

Keep ransomware policies up to date.

Regulations are also being formulated in areas such as reporting ransomware attacks and even making it a crime to pay a ransom. Company policies regarding paying ransomware need to be reviewed, along with likely changes to cyberinsurance policies.

Prepare for required "Software Bill of Materials" in order to better vet your digital supply chain.

Many companies did not know that they had the log4j vulnerability in their systems because that software was often bundled with other software that was bundled with other software. There are regulations being proposed to require companies to maintain a detailed and up-to-date Software Bill of Materials (SBOM) so that they can quickly and accurately know all the different pieces of software embedded in their complex computer systems.

Although an SBOM is useful for other purposes too, it may require significant changes to the ways that software is developed and acquired in your company. The impact of these changes needs to be reviewed by management.

What More Should You Do?

Someone, or likely a group in your company, should be reviewing these new or proposed regulations and evaluate what impacts they will have on your organization. These are rarely just technical details left to your information technology or cybersecurity team — they have companywide implications and likely changes to many policies and procedures throughout your organization. To the extent that most of these new regulations are still malleable, your organization may want to actively influence what directions these regulations take and how they are implemented and enforced.

Acknowledgement: This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.