451 Research

S&P Global
Market Intelligence

The conflict in Ukraine may indirectly trigger more cybersecurity investment

Analysts - Daniel Kennedy

Publication date: Tuesday, March 29 2022

Introduction

The Strengthening American Cybersecurity Act of 2022 was signed by President Joe Biden on Tuesday, March 15. The primary takeaway of the Act is that organizations that maintain critical infrastructure must report substantial cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) no later than 72 hours after determining an incident has occurred. Organizations must also report any ransomware payment made within 24 hours.

The new law follows an executive order issued on May 12, 2021, focusing on the protection of federal government IT infrastructure. That order was directly linked to both the SolarWinds and Colonial Pipeline attacks and focused on protecting software supply chains and requirements around Software Bills of Material. This latest legislation also has roots in the Colonial Pipeline attack and focuses on strengthening CISA, but the urgency in its passage can be tied directly to the threats posed by the escalating tension between the US and Russia over the conflict in Ukraine.

The Take

A question often asked relevant to the conflict in Ukraine is whether the potential for an offensive cyberattack by Russia against the US in response to economic sanctions and military aid would spur US-based companies that maintain critical infrastructure to invest more in cybersecurity. There certainly will be some investment that can be directly tied to the conflict; security leaders in organizations considered to be critical infrastructure will likely leverage changes in the threat landscape to convince business leadership of the wisdom of certain expenditures. President Biden's statement of March 21 encourages that conversation, laying out that private industry can be thrust into the sometimes uncomfortable role of national defense, especially when it comes to cyberattacks. A greater trigger for investment may be a step downstream from the conflict, however, and that is the expansion of breach notification requirements for critical infrastructure outlined in the recently signed Strengthening American Cybersecurity Act of 2022.

Historical context of breach notification laws

California Senate Bill 1386, enacted in 2002, kicked off the passage of similar state laws requiring companies to disclose a data breach to customers in writing, and as such remains one of the most impactful shifts in the history of cybersecurity. No longer could breaches of customer data be a private affair for a company, and disclosure carried with it direct costs of customer communications and resolutions such as paying for credit monitoring, but also downstream costs such as customer loss, lawsuits and reputational damage. Companies were presented with a direct incentive toward minimizing information security risks, and at least maintaining some capability in determining what happened after a successful cyberattack. The significant impact of notification laws, and a desire to avoid the downstream expense they create, can correlate fairly directly to information security investments.

CISA's aim, and potential issues for private business

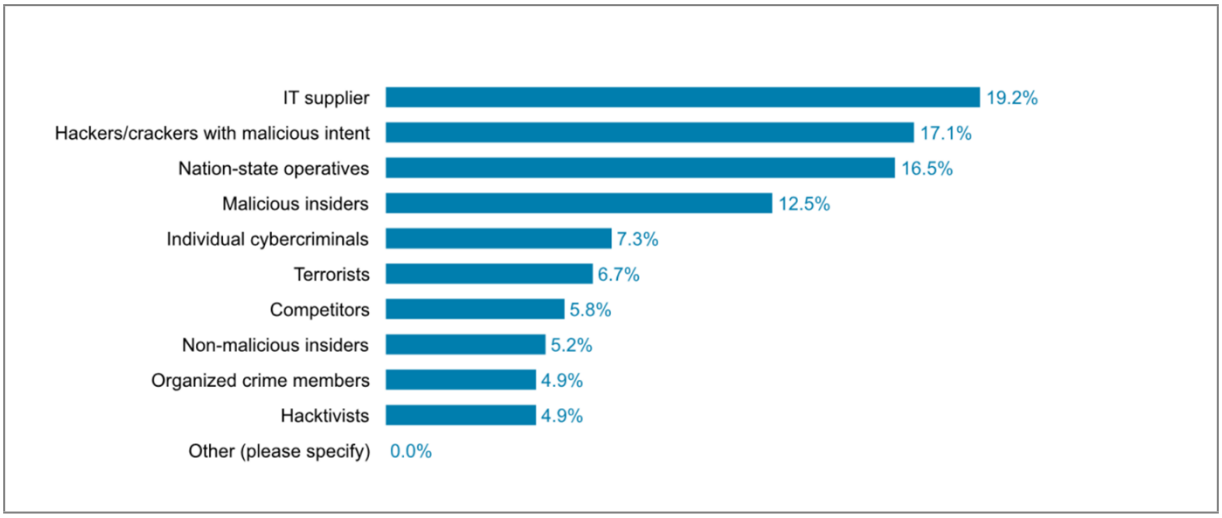
There's nothing new in promoting the sharing of security threat information among public and private critical infrastructure operators; some of the earliest ISACs (Information Sharing and Analysis Centers) were formed in 1999 in response to Presidential Decision Directive-63 (PDD-63). Separating this from earlier efforts, the approach outlined here involves penalties for non-compliance, including the ability of the CISA Director to issue subpoenas to compel disclosure. Not responding to a subpoena has the potential to bring on a civil action by the Attorney General. The value to CISA is clear; it can bring resources to bear and accurately report on an attack on private infrastructure that puts public interests in jeopardy, as well as identify patterns across multiple different enterprises being attacked.

That said, while CISA is identified as the lead in such investigations, part of the mandate is information sharing with other federal entities and information sharing organizations (e.g., the abovementioned ISACs). So first, there is a greater potential for the information leaking to the public, and second, some of the data may be a public records request away for many journalists. This quickly becomes, in practice, a breach notification to the market that did not exist previously (where customer personal information was the focus of such laws).

As noted earlier, history tells us that many organizations seek to avoid such notifications, and they become a driver of getting one's cyber defense in order as part of that risk avoidance where possible. Where it isn't possible, having an information security program that is at least defensible in the face of public scrutiny, despite having a problem, becomes the requirement. Not all attacks can be defended; as noted in the figure below; there is a class of threat associated with government funding and resourcing, historically called an advanced persistent adversary (APT) where detection and response become key attributes of a security program over prevention.

It is also reasonable to wonder whether the combination of having to report ransomware payments in a semi-public manner, the escalating ransom amounts being demanded and the insurance industry's partial retreat from offering coverage for such attacks will result in fewer ransoms being paid as the cost-benefit calculation of handing money over to attackers changes. Government entities at all levels, for their part, are attempting to discourage such payments as that funding enables a continual profitable enterprise for bad actors; however, that interest may not supersede a business's desire to get back up and running as soon as possible because downtime has a very tangible cost as well.

Sources of Threats That Cybersecurity Teams Believe They Are Least Prepared to Counter



Source: 451 Research, Voice of the Enterprise: Information Security, Organizational Dynamics 2021
Q Which one of the following sources is your organization least prepared to deal with as a data security threat?
Base: All respondents, abbreviated fielding (n=328)