Institute for SECURITY + TECHNOLOGY

October 28, 2021

Dear Member of Congress:

The undersigned organizations and representatives urge you to support forthcoming legislation that implements mandated reporting requirements for cyber incidents and in the event an organization makes a ransomware payment.

Cyber incidents are economically destructive and can have serious repercussions that ripple across industries. The effects of these incidents are only worsening as governments and businesses increasingly rely on complex technological systems and threat actors shift to target critical infrastructure like supply-chains, power grids, schools, and hospitals. We expect these threats will only continue to grow in severity and with physical consequences over the next several years. While well-crafted reporting requirements do not solve these security challenges, they can greatly increase our collective ability to defend against these types of attacks—and prevent continued economic, societal, and broad-scale public health damage.

Need For Mandated Cyber Incident and Ransomware Reporting Requirements:

Mandatory incident reporting requirements are not unprecedented. In fact, the banking and financial services sectors already have mandated reporting for cyber incidents. Developed over nearly 20 years and supported by several instances of congressional legislation (i.e. the **Gramm-Leach-Bliley Act**), the requirements were introduced after a number of infamous data breaches scattered troves of private, financial, and sensitive information across the illicit web.

In recent years, attacks against the oil and gas industry, the food processing industry, hospitals, and transportation networks have all increased. Additionally, the ever-increasing role of third-party software providers has created complex technology supply-chains that transport private, financial, and sensitive data across a wide landscape of actors. Therefore, as criminal cyber actors have expanded their activity beyond the financial sector, the need for broader cyber incident reporting requirements has also grown.

Experience has clearly shown that too few companies voluntarily report cyber incidents to the U.S. Government. As a result, without mandated incident reporting requirements, the U.S. Government cannot fully perform its cybersecurity mission. As highlighted by CISA Director Easterly in Senate committee hearings earlier this year, prompt reporting can help CISA and other agencies move more quickly to support victims, as well as identify and warn other exposed organizations. It would also provide the Federal Government with better data regarding the scope, scale, frequency, and distribution of cyber incidents. In turn, this data would enable the Federal Government to allocate its resources more efficiently and to target malicious cyber actors for disruption more effectively.

Impact of Mandated Cyber Incident and Ransomware Reporting Requirements:

The benefits of mandatory reporting would not just accrue to the Federal Government. Properly crafted reporting requirements would also generate benefits for the private sector. For example, companies reporting cyber incidents would then be able to access federal resources, increasing the chances of asset and ransom recovery. Companies would also use the existence of mandatory reporting requirements as a justification for increasing their baseline level of cybersecurity to reduce the likelihood of having a reportable cyber incident in the first place. This outcome would be especially important for small businesses that may not have the same capabilities for incident response as large organizations and are especially placed in a precarious position as victims of a malicious cyberattack.

By designing simple, easy to comply with reporting requirements for small businesses, Congress can effectively ensure that all businesses have equitable access to the vast array of resources offered by the U.S. Government, while still not overburdening small businesses. Such comprehensive reporting requirements would also ensure that we have the most accurate, broadest representation possible of the actual threat in order to best be positioned to combat it. Finally, if the Federal Government makes aggregated, anonymized versions of the reported data available to the private sector, then this reporting would help organizations prepare for similar incidents or attacks.

The **Ransomware Task Force (RTF) report**, released earlier this year, highlights positive incentives that come with mandatory reporting. This includes increasing implementation of cyber hygiene within an organization, improving collaboration between the U.S. Government and private sectors, as well as providing an important safety net to victims of attacks.

The RTF report also highlighted the importance of incorporating limited liability protections, including the stipulation that the report cannot form the basis of regulatory or other enforcement actions as a result of those mandatory reporting requirements. This limitation will ensure that organizations remove regulatory or enforcement worries when calculating the next steps after a ransomware incident. In this way, the U.S. Government provides net support to impacted organizations, and incentivizes further collaboration to respond to incidents, recover critical services, and hold cybercriminal actors accountable.

Conclusion:

Mandatory reporting will increase transparency, improve threat mitigation capabilities across sectors, aid in the ability to discover and patch vulnerabilities, and help identify and pursue cyber criminals. As a result, mandatory reporting will help all parties mitigate cyber threats in the long run and reduce the threats posed to the people, businesses, and critical infrastructure of this country.

We urge support of these mandated reporting requirements.

Sincerely,
The undersigned:

Philip Reiner
Institute for Security and Technology

Michael Daniel
Cyber Threat Alliance

Chris Painter

Megan Stifel