wiley

NEWSLETTER

10 Ways the Ransomware Task Force's New Report Could Impact the Private Sector

May 2020

Privacy In Focus®

In the last few years, thousands of businesses, hospitals, school districts, local governments, and other entities have fallen victim to ransomware. Several government and quasi-government groups are looking to take action. The Institute for Security and Technology's (IST) Ransomware Task Force (RTF) recently offered several notable recommendations that will affect the private sector if adopted.

On April 29, the RTF – a coalition of volunteers from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations – released a report titled *Combating Ransomware* (Report), which provides a framework for addressing ransomware's proliferation. The RTF defines ransomware as a form of cybercrime through which criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data. As the RTF explains, ransomware is a flourishing criminal industry that not only threatens the personal and financial security of individuals, but also puts national security and human life at risk.

The Report offers 48 recommended actions for both government and industry to disrupt the ransomware business model and mitigate the impact of ransomware attacks going forward. The Report is organized around four Goals, each of which contains several general Objectives and specific Actions:

1. ***Deter*** ransomware attacks through a nationally and internationally coordinated strategy;

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kyle M. Gutierrez
Associate
202.719.3453
kgutierrez@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

2. ***Disrupt*** the ransomware business model and reduce criminal profits;
3. Help organizations ***prepare*** for ransomware attacks; and
4. ***Respond*** to ransomware attacks more effectively.

Early responses to the Report indicate that it may have a broad impact, as the federal government appears to be taking the RTF's recommendations seriously. For example, a few hours after the Report's release, U.S. Department of Homeland Security (DHS) Secretary Alejandro Mayorkas stated that the Report "will help guide a whole-of-government approach to the problem of ransomware," adding that the White House is working on its own plan to combat ransomware as well. Given this interest, below we identify 10 key recommendations in the RTF Report that could directly impact the private sector.

(1) Require Organizations and Incident Response Entities to Share Ransomware Payment Information with a National Government Prior to Payment

The Report recommends that data breach disclosure laws be updated to include a pre-ransom payment disclosure requirement, in order to increase the understanding of the scope, scale, and impact of, and best ways to disrupt, ransomware attacks. The Report explains that this requirement to report prior to payment would also enable national governments to take defensive actions and help organizations understand how to develop their preparative measures.

Under this requirement, the Report explains, organizations should be required to report to a non-regulatory agency prior to payment, which in turn would then share the information with other appropriate non-regulatory agencies and (after anonymization) the RTF's recommended Ransomware Incident Response Network (RIRN). The RIRN will be explained in greater detail in Recommendation Five. The Report recommends that organizations should be required to provide the ransom date, demand, payment instructions (e.g., wallet number and transaction hashes), and amount. However, organizations should also be able to provide additional technical information when they can and use insurance providers or incident response entities to report on their behalf.

(2) Require Organizations to Review Alternatives Before Making Payments

The Report recommends that organizations should be obligated to review their alternative options before making a ransom payment. The Report explains that this requirement would allow organizations to push back on demands for immediate payment and would reveal the viability of options between payment and rebuilding their network from scratch. The Report further expresses that these reviews should be scaled to the size and criticality of the organization – for instance, such a review might only consist of two or three actions for small and medium-sized businesses.

(3) Require Organizations to Conduct a Cost-Benefit Analysis Prior to Making Payments

The Report recommends that medium and large organizations should be required to conduct and document a cost-benefit analysis prior to making or authorizing any ransom payments. To facilitate this requirement, the Report also recommends that a standard cost-benefit analysis matrix be developed, which would also allow for inter-organization comparisons and data collection.

(4) Establish a Private-Sector-Led Ransomware Threat Focus Hub

The Report recommends that relevant private-sector organizations – including security vendors, platform providers, telecommunications providers, information sharing organizations, and cybersecurity nonprofits – should come together to operate a Ransomware Threat Focus Hub (RTFH). The RTFH would collaborate closely with the government-led Joint Ransomware Task Force (JRTF) to help fight back against ransomware operations.

The Report explains that the RTFH should serve as a central, organizing node for informal networks and collaboration as part of a public-private anti-ransomware campaign. Among other things, the RTFH would facilitate and coordinate sustained private-sector actions against an agreed-upon target list, in coordination with the government's JRTF.

(5) Establish a Ransomware Incident Response Network

The Report recommends that an array of public and private organizations agree to share information rapidly and in standardized formats as part of a Ransomware Incident Response Network (RIRN). Among other things, the RIRN would foster the sharing of ransomware incident reports, direct organizations to assist with incident response, aggregate data, and issue alerts for ongoing threats.

The Report explains that the RIRN should consist of nonprofit organizations; for-profit entities (including cybersecurity vendors, insurance providers, and incident responders); and national government agencies and law enforcement.

(6) Establish a Voluntary Insurance Sector Consortium

The Report recommends that the insurance sector establish a voluntary consortium to share ransomware loss data and develop best practices around insurance underwriting and risk management in this area. The Report also suggests that this consortium work directly with both the JRTF and RTFH.

(7) Require More Stringent Compliance from Cryptocurrency Entities

The Report argues that many cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" are not consistently compliant with or subject to Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) requirements. This can help facilitate ransomware attacks, which usually rely on payment in cryptocurrencies. Thus, the Report recommends that enforcement be increased, and also that financial institutions that fund these entities impose stricter due diligence and pursue SEC enforcement of the entities that fail to register themselves properly.

(8) Highlight Available Anti-Ransomware Internet Sources

The Report recommends that, as they did with materials related to COVID-19, internet search companies should prioritize ransomware-related materials on their search pages. Specifically, the Report emphasizes that a ransomware mitigation, response, and recovery framework should be developed and implemented internationally, as this could be the single most impactful measure that could be taken to help organizations combat ransomware attacks. Internet search companies should thus prioritize this framework and other complementary materials. The Report explains that this would make sorting through online materials easier and thus decrease the confusion and complexity surrounding the ransomware problem.

(9) Update Existing Cyber-Hygiene Regulations and Standards

Although there are several cybersecurity regulations and standards – both domestically and internationally – that set a baseline for cybersecurity in specific sectors, the Report authors argue that these regulations and standards do not sufficiently account for ransomware. As such, the Report recommends that these regulations and standards be updated to incorporate measures that align with the Report's other recommendations to more directly confront ransomware.

(10) Managed Service Providers to Adopt and Provide Baseline Security Measures

The Report argues that managed service providers (MSPs) do not usually provide extensive security coverage or ransomware mitigations. The Report recommends that MSPs should change course and adopt baseline security measures to include: (a) adherence to a cyber-hygiene program; (b) mandatory disclosure of a ransomware incident across the MSP's customer base; and (c) forming an MSP information sharing and analysis center specific to this industry. The Report argues that this would benefit small to medium-sized organizations.

Unfortunately, the ransomware threat does not appear to be going away anytime soon. As such, the government is sure to take additional steps to attempt to stem the tide of these attacks. The RTF Report's recommendations will likely influence the federal government's approach, and organizations of all shapes and sizes will want to keep an eye on developing obligations and expectations in dealing with ransomware threats.

Wiley recently addressed some of the steps that in-house counsel can take to help manage their organization's approach to potential ransomware attacks in the February edition of *Privacy In Focus*. If you have any questions or would like any additional information about what you or your organization can and should be doing to address the ransomware threat, please do not hesitate to contact one of the members of our Privacy, Cyber & Data Governance group.