Making Practical Use of the Federal Agencies' New Ransomware Guidance

May 26, 2023

Categories:

Blogs
Technology Blog

Authors:

William T. Repasky
Robert W. Dibert
Gene F. Price

Business leaders will find important information in the *#StopRansomware Guide* developed through the U.S. Joint Ransomware Task Force and issued May 23, 2023. The guide is primarily a technological review of best practices that businesses may implement to avoid becoming a victim of ransomware. However, it has other non-technology recommendations that we believe are at least equally important to business leadership.

#StopRansomware presents a holistic approach to confronting the risk posed by ransomware. Part 1 of the guide, and its primary focus, addresses cybersecurity technology issues, such as the "initial access vectors" exploited by criminal ransomware as a service (RaaS) affiliates to implant the malicious encryption software, and approaches for hardening a company's cyber defenses.

Part 2 focuses on ransomware response strategies. This is of specific import for business leaders and others responsible for protecting the company's reputation and/or leading its "Incident Response Team." Located in Point #7 of Part 2 is the somewhat vague, and likely purposefully so, recommendation to build a plan "to engage internal and external teams and stakeholders." It is our belief that this is one of the most critical aspects to every incident response plan! The effective planning and execution of a company's communications and notifications plan will likely yield the greatest benefit to the company in terms of minimizing the overall direct and indirect costs that unfortunately flow from every ransomware attack.

When our team participates in incident response plan creation and training, we place emphasis on what we term the "Communication Matrix." First of all, the Communication Matrix should be built with the leisure of an unpressured environment. In other words, determining exactly who the company must communicate with should not occur in the firestorm of an actual ransomware attack.

FBT Gibbons

#StopRansomware speaks about internal and external stakeholders. The Incident Response Team's first objective is to identify who are all the company's stakeholders to be detailed in the Communication Matrix. That list will commonly include all members of the Incident Response Team, the board of directors, senior management, employees, key customers and core third-party vendors. Additionally, the company's insurance providers are vital stakeholders, as are law enforcement and any prudential regulator, if any, within the company's industry.

Once the full list of stakeholders is created, then the Communication Matrix is built out in a spreadsheet type of format. For each stakeholder identified, the matrix must be completed to identify the "WHO," being the specific contact person for each stakeholder and contact information for each of those individuals or their substitutes. A ransomware attack is not the time to be searching for your FBI field office's phone number(s), for example. The next column on the matrix will be the "WHY." Here will be detailed the legal basis or the business reason for why this stakeholder is recognized in the matrix. For example, certain industries are required by federal and/or state law and regulations to provide notification to specific agencies in the event of a material cybersecurity incident.

The "WHAT" column in the Communication Matrix identifies the scope and content of what must be communicated, at least initially. With foresight, the actual details of what the company is legally required to communicate and/or business-related information will be memorialized in the matrix. The important "WHEN" column is completed with the specific deadline(s) applicable to each stakeholder. By way of example, financial institutions operate under a 36-hour notification deadline after discovery of a material computer-security incident. Not only will this information assist in making sure that no deadlines are overlooked, but this information will permit the company to best allocate its (nearly always) limited resources during a ransomware attack.

The next column of the Communication Matrix is the "HOW" information. Specifically, how is each required notification to be made, such as by phone call, in writing or otherwise. The last

element of information commonly included is “WHO #2,” which identifies exactly who from the company will be responsible for the communication task required.

There is no one-size-fits-all formula for an effective Communication Matrix. The facts and circumstances of each company vary, as do the legal environment in which each operates. And this document requires diligent maintenance. Stakeholders commonly change over time, as might the details linked to each of them. For example, the Cyber & Infrastructure Authority (CISA) now is engaged in rulemaking that soon may require all “critical infrastructure” businesses to report certain cyber incidents within 72 hours and ransomware payments within 24 hours.

The goal and purpose of the Communication Matrix is to bring intentionality and prioritization to the company’s communication efforts. Controlling the messaging is of vital concern to protecting brand reputation. Equally important, understanding the who, what and when of your communication strategy ensures that compliance deadlines are not missed or that stakeholders are not left in the dark through oversight. A ransomware attack can create a chaotic environment, but having a well-considered Communication Matrix will bring a measure of confidence and assurance.

Related to the concept of the Communication Matrix is the advance planning that the Incident Response Team must accomplish to ensure that communication channels among its members remain open and secure during a ransomware event. A wide-ranging ransomware attack often renders inoperable the company’s email system. In such cases, has an alternative procedure been planned for in advance to allow the team to remain in constant communication with each other? Similarly, if the extent of the threat actor’s intrusion or privileges are unknown, how confidential is the communication channel being used by the Incident Response Team to make important remedial decisions?

For additional information about building your company’s strategy for confronting and mitigating the damages of a ransomware attack, please contact Bill Repasky, Bob Dibert, Gene Price, or any attorney with Frost Brown Todd’s Data Security & Privacy team.

FBT Gibbons

FBT Gibbons