PROTECT YOUR BUSINESS

Ransomware Alert

think again, and then again

By Christopher Scott D'Angelo

Many contractors and other businesses do not even think about it and if they do, they think it is something only the Fortune 500s of the world need worry about. This delusion is extremely dangerous and short-sighted. As the FBI, U.S. Secret Service, and the Cybersecurity and Infrastructure Security Agency repeatedly warn, ransomware attacks have an impact upon all sectors, and many ransomware attacks also target small- and medium-size businesses. According to the FBI's 2018 and 2019 Internet Crime Reports, there was a 37% annual increase in reported ransomware cases and a 147% annual increase in associated losses from 2018 to 2019. Particularly targeted at present is the infrastructure and the expansion of construction projects occurring under the infrastructure programs of the federal government.

FORMS OF RANSOMWARE

Ransomware is a form of malicious software—malware—designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from their targets in exchange for the key to decrypting the information and restoring the target's access to their systems or data. The "cybercriminals" use stealth, phishing and creative schemes to introduce the malware into the target's systems, taking advantage of gaps or weaknesses in the electronic systems or, in fact, ignorance, laziness or mere inattention of the targets. As the U.S. National Cyber Investigative Joint Task Force states, common infection mechanisms include:

Email phishing campaigns: The cybercriminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cybercriminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cybercriminal to use a victim's email account to further spread the infection.

Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cybercriminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware, including ransomware, to victim systems.

Software vulnerabilities: Cybercriminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

In addition to the attack, the cybercriminals often threaten to publicly disclose victims' sensitive files. The Cybercriminals then demand a ransomware payment, usually through digital currency, in exchange for the decryption key.

ELECTRONIC OPERATIONS

Contractors increasingly rely on electronic systems and the exchange of contracts, subcontracts, vendor communications, designs, drawings and specifications, and shared documents and data, but like many businesses, contractors often do not have a true IT or in-house network security staff, thus making them more susceptible than average to such ransomware cyberattacks. And even average is nowhere near good enough.

The economic and reputational damage caused by ransomware incidents, whether from the initial disruption or through the often-extended recovery, can be extensive. Not only will ransomware incidents severely impact the contractor's operations, but by forcing it to shut down during the attack, the contractor cannot perform and becomes potentially subject to liability to the owner for the delays, missed benchmarks, additional supply costs, or other breach of contract.

DANGER OF RANSOMWARE

Victims of such ransomware cyberattacks often think they should—or have no choice but to—just pay the ransom. This is an understandable reaction, but it is fraught with serious dangers, and not merely dealing with despicable and dishonest actors who may or may not live up to freeing the captive system and data and may or may not slip a stealth sleeper file or backdoor for a later attack or the theft of data.

In fact, paying or facilitating ransomware payments may subject the victim and those assisting the victim

to significant criminal or civil penalties. For example, as the Department of the Treasury notes, "ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden Cybercriminals to engage in future attacks." Such activities may also be subject to restrictions and liability under the International Emergency Economic Powers Act or the Trading with the Enemy Act, Executive Orders, and Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons List, among others.

PROTECTING YOUR BUSINESS

What should the contractor do? First adopt and maintain detailed protective policies or systems and remember to review your contracts, particularly the force majeure and limitations of liability clauses to be sure that they protect you in the event of delays, disruptions and other effects of a ransomware attack or other cyberattack not only on your company but also on all those whom you work with on the project.

In addition, contractors and other businesses should investigate insurance options. The right insurance can help reduce concerns about ransomware attacks. The challenge is finding affordable coverage. According to Marsh, in 2021 cyber insurance pricing in the United States increased an average of 96% year-over-year. Insurers are also insisting on more staff and updated systems. In looking for insurance, the business should be looking for and considering coverage for business interruption, data recovery, security incident and breach coverage, and dependent business interruption relating to supply chain risks. Companies should also look for insurers that provide support and service.

CLOSING THOUGHT

The cliché is "an ounce of prevention is worth a pound of cure." Here, it is more, an ounce of prevention can save your assets. Act now. ■

ON THE WEB

More resources and contacts are in this article on mcsmag.com

about the author

Christopher Scott D'Angelo is chair of both the Business Disputes & Products Liability Practice and International Practice at Montgomery McCracken Walker & Rhoads LLP, based in Philadelphia and New York City. His practice involves business, products liability, construction, class action, and insurance counseling and litigation, including his role as national counsel for several major U.S. clients and his representation of foreign concerns in the United States and U.S. concerns abroad. He can be reached at cdangelo@mmwr.com.