7-Nextgov-Colonial Pipeline

Colonial Pipeline Forked Over $4.4M to End Cyberattack – But Is Paying a Ransom Ever the Ethical Thing to Do?

glegorly/iStock.com

Get the latest federal technology news delivered to your inbox.

email

By Scott Shackelford and Megan Wade , The Conversation

By Scott Shackelford and Megan Wade , The Conversation

May 28, 2021

Cyber Threats

It took little over two hours for hackers to gain control of more than 100 gigabytes of information from Colonial Pipeline on May 7, 2021 – causing the firm to shut down its fuel distribution network and sparking widespread fears of a gasoline shortage. The decision to pay off the attackers was also made with apparent speed , but the ethical arguments involved are age old and the implications could reverberate well into the future.

Cyberattacks, including those on critical infrastructure in the U.S., are nothing new. Ransomware, a type of malicious software that locks access to a computer until a ransom is paid, has been a component of the cyberthreat landscape since the mid-2000s. But the Colonial Pipeline breach raised the stakes and highlighted the ability of ransomware to interrupt the vital services on which Americans rely.

As scholars of cybersecurity policy , in particular critical infrastructure protection and ransomware , we think it important to consider the legal and ethical questions surrounding ransomware payments – just because paying

off cyberattackers may be lawful in some contexts, that still doesn't make it the morally correct thing to do.

To Pay or Not to Pay

It has been widely reported that the Colonial Pipleline CEO Joseph Blount agreed to pay a US$4.4 million ransom to DarkSide *[Compliance]* , the Russia-based group behind the cyber attack.

In describing his decision, which he said did not come lightly, Blount argued that it was justifiable given that it was "the right thing to do for the country *[Reinforce]*."

Official guidance suggests otherwise. *[Worry]* In October 2020, the Treasury Department warned that ransomware payments are a violation of its rules and would only encourage future demands. Although there is no federal legislation, such states as California, Texas and Michigan have cyber-extortion laws on the books that discourage ransomware payments.

Often, though, the decision of whether to pay falls in a legal and ethical gray area.

CEOs can turn to three main schools of ethics in guiding decisions about whether to pay ransoms based on virtues, duties and consequences.

Under virtue ethics , which traces its origins to philosophers Plato, Aristotle and Confucius, people make decisions based on a set of virtues or character traits such as honesty and loyalty. In and of itself, the tradition does not help in situations that require weighing one virtue against another, such as not wishing to reward criminal activity against preventing disruption to the wider American public. For example, Colonial Pipeline CEO Blount expressed a moral distaste in paying "people like this," but ultimately decided to override that concern based on other factors.

Another way to approach challenging ethical decisions is through what is called the deontological approach , which holds that actions are good or bad determined by a clear set of rules. So another way to come at the question

of whether to pay a ransom is to ask, “How does doing so align with recognized universal duties?”

The problem with cybersecurity is that, given the rapidly changing technological and regulatory environment, it is not always clear what the “golden rules” are, or even if any have been established. Some business leaders may even perceive a duty to pay as Blount did, especially in the case of critical infrastructure such as pipelines on which so many people rely.

The ethics of ransomware payments can also be viewed through the consequences of the decision to yourself, your family, your ganization and, as Blount suggested, the country and the world. Utilitarian philosophers hold that what is important is promoting the greatest good for the greatest number of people.

This is often described in boardrooms and policy circles as cost-benefit analysis. Yet it’s not always clear where to put that next dollar of investment to maximize the good and minimize the harm in the long term. In dealing with ransomware, for example, backing up data is key, as is practicing zero-trust security , an approach in which companies assume that their networks are already compromised and act accordingly. But doing so can be complex, and investments might cause fewer benefits than if the money were invested elsewhere.

Pros of Paying

In practice, business leaders use all these ethical tools, and more, in deciding whether or not to pay – and there isn’t much time to weigh the options. Colonial Pipeline CEO Blount’s decision reportedly came almost immediately .

And it isn’t universally accepted that Colonial Pipeline came to the right decision.

[Disappointment]

Some cybersecurity professionals want to ban paying out ransoms to halt the growing problem of malware attacks for profit . Others say banning payments would be a “ horrific game of chicken ” in which cyberattackers up the stakes until the consequences of not breaking the law are greater for the companies involved than the impact of the breach. And banning ransom payments outright would place an impossible burden on smaller businesses or organizations that do not have the resources to protect against malicious actors.

The thinking behind banning payments is that attacks might stop if they don’t yield payments. Yet if the attack has the capability of paralyzing an entire entity, paying up is often the economically rational decision in the short term . An attack on the Irish Healthcare System in May, for example, is expected to cost tens of millions of euros to rebuild the network . Cybersecurity experts estimate that companies hit by attacks take an average of 287 days to fully recover to normal operations .

Ransomware as a Service

The rapid proliferation of attacks has been fueled by a new business model known as “ransomware as a service.” Ransomware developers sell personalized variants to “ affiliates ” – cybercriminals who deploy the ransomware .

With the emergence of ransomware as a service, ransomware can be profitable for both the developers of the variant and the affiliates.

Not all affiliates and ransomware developers are governed by the same moral code. DarkSide, which conducted the Colonial Pipeline attack, has its own set of principles, which include not attacking certain targets, such as medical services, the educational establishment and nonprofit organizations .

DarkSide has also been known to promise it will completely leave a network alone after ransom is paid .

The FBI discourages payment, partly on the grounds that it is not a guarantee that a company will not be hit again.

But the message is mixed. Law enforcement agencies encourage victims not to pay, but paying ransom is not illegal, and even police departments have been known to pay up when their systems have been compromised. And while the Treasury Department has been investigating new financial penalties against payment of ransoms, to date none have been levied .

But even without the threat of legal sanction, payment of ransomware will continue to pose a moral dilemma.

Scott Shackelford is an associate professor of business law and ethics; executive director, Ostrom Workshop; and cybersecurity program chair at IU-Bloomington, Indiana University. Megan Wade is a Research affiliate at the Ostrom Workshop for Cybersecurity and Internet Governance at Indiana University.

Do Not Sell My Personal Information

When you visit our website, we store cookies on your browser to collect

information. The information collected might relate to you, your preferences or your device, and is mostly

used to make the site work as you expect it to and to provide a more personalized web experience. However, you

can choose not to allow certain types of cookies, which may impact your experience of the site and the

services we are able to offer. Click on the different category headings to find out more and change our

default settings according to your preference. You cannot opt-out of our First Party Strictly Necessary

Cookies as they are deployed in order to ensure the proper functioning of our website (such as prompting the

cookie banner and remembering your settings, to log into your account, to redirect you when you log out,

etc.). For more information about the First and Third Party Cookies used please follow this link.

Allow All Cookies

Manage Consent Preferences

Strictly Necessary Cookies - Always Active

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy

choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of

your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts

of the site will not work as intended if you do so. You can usually find these settings in the Options or

Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data, Targeting & Social Media Cookies

Under the California Consumer Privacy Act, you have the right to opt-out of the

sale of your personal information to third parties. These cookies collect information for analytics and to

personalize your experience with targeted ads. You may exercise your right to opt out of the sale of personal

information by using this toggle switch. If you opt out we will not be able to offer you personalised ads and

will not hand over your personal information to any third parties. Additionally, you may contact our legal

department for further clarification about your rights as a California consumer by using this Exercise My

Rights link

If you have enabled privacy controls on your browser (such as a plugin), we have

to take that as a valid request to opt-out. Therefore we would not be able to track your activity through the

web. This may affect our ability to personalize ads according to your preferences.

Targeting cookies may be set through our site by our advertising partners. They

may be used by those companies to build a profile of your interests and show you relevant adverts on other

sites. They do not store directly personal information, but are based on uniquely identifying your browser and

internet device. If you do not allow these cookies, you will experience less targeted advertising.

Social media cookies are set by a range of social media services that we have

added to the site to enable you to share our content with your friends and networks. They are capable of

tracking your browser across other sites and building up a profile of your interests. This may impact the

content and messages you see on other websites you visit. If you do not allow these cookies you may not be

able to use or see these sharing tools.

If you want to opt out of all of our lead reports and lists, please submit a

privacy request at our Do Not Sell page.

Save Settings

Cookie Preferences Cookie List

Cookie List

A cookie is a small piece of data (text file) that a website – when visited by a

user – asks your browser to store on your device in order to remember information about you, such as your

language preference or login information. Those cookies are set by us and called first-party cookies. We also

use third-party cookies – which are cookies from a domain different than the domain of the website you are

visiting – for our advertising and marketing efforts. More specifically, we use cookies and other tracking

technologies for the following purposes:

Strictly Necessary Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy

choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of

your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts

of the site will not work as intended if you do so. You can usually find these settings in the Options or

Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Functional Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our

website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site

performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You

can set your browser to block or alert you about these cookies, but some parts of the site will not work as

intended if you do so. You can usually find these settings in the Options or Preferences menu of your

browser. Visit www.allaboutcookies.org to learn more.

Performance Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our

website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site

performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You

can set your browser to block or alert you about these cookies, but some parts of the site will not work as

intended if you do so. You can usually find these settings in the Options or Preferences menu of your

browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.

Social Media Cookies

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.

Targeting Cookies

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.