Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Evaluating Ethical And Legal Risk In Ransomware Payments

By **Rob Dedman and Kim Roberts**

Robert Dedman

Kim Roberts

Law360 (January 14, 2021, 3:08 PM EST) -- As we enter 2021, the costly risk of cybersecurity breaches is back on the agenda once more.

Not only do U.K. businesses face a cyberattack every 46 seconds, according to a recent report from specialist internet service provider Beaming Ltd., but it was recently reported in the press that Ryuk, a ransomware outfit, has raked in more than £110 million (approximately $150.5 million) via its attacks. A lucrative, and illegal, business indeed.

Meanwhile, the list of entities facing cyberattacks in the last few weeks has added construction giant Amey PLC, Hackney Council in London and technology outfits SolarWinds Worldwide LLC and AKVA Group ASA, while the privacy group action against British Airways PLC for its 2018 breach has attracted more than 16,000 claimants.

When dealing with ransomware incidents, most companies — both in the financial services industry and beyond — have a no-pay policy: They will not pay to release systems locked down by ransomware. And with good reason — payment is a risky business from almost every position you approach it.

Practically, you never know whether payment is really going to lead to systems being unlocked or just a demand for further payment. Reputationally, it is seen by many as being ethically suspect. From a legal and regulatory perspective, you are potentially skating on thin ice, both in terms of sanctions regulations, and more generally with some regulators, particularly in the U.S., who are increasingly keen to ensure that cybercrime doesn't pay.

And there is the inevitable moral hazard: Once cybercriminals know that you have paid once, there's always the risk of open season.

But what if the incident is so severe it threatens the very existence of the company? Is the line more blurred in that context, and can the no-pay policy survive in that environment?

What Is Ransomware?

Ransomware is malicious software used by cybercriminals to deny availability or access to systems or data. After the threat actors gain access to a network, they deploy ransomware to shared storage drives and other accessible systems. They then hold the data or the system hostage until their demands are met, during which period the system or encrypted data is unavailable or may be deleted, and in some cases threaten to publicly disclose the data if the ransom is not paid.

Ransomware attacks, alongside most other forms of cyberattack, are on the rise. The results of a survey carried out in late 2019 and early 2020 by the U.K. government reported that among the 46% of businesses that identified breaches or attacks, one in five, or 19%, experienced a material outcome, losing money or data. Two in five, 39%, were negatively impacted, for example requiring new measures, having staff time diverted or causing wider business disruption.

When Is the Business at Risk?

Financial services firms often invest significantly in strong security measures and are well protected, but periods of organizational changes such as the increased home working arrangements that firms have had to deploy rapidly and on a significant scale during the COVID-19 pandemic have made many firms more vulnerable to cyberattacks.

Furthermore, suppliers are also susceptible to attacks. Third parties critical to remote operations are now attractive targets. A ransomware attack against a third party could disrupt a large institution or multiple institutions and impact the wider economy.

As such, strong systems and controls for onboarding, overseeing and dealing with incidents at third-party suppliers are vital to ensure a firm's infrastructure is protected from all angles. Financial regulators, in particular, regard operational resilience, particularly in relation to outsourced services, as critical to an appropriate control environment.

Assessing all Risks

We are frequently asked by clients that are the victims of a ransomware attack: What if we were to consider payment? What are the risks? Would we have to disclose to regulators or to the public?

Our baseline approach is generally to recommend that clients view payment of any demand for ransom as a last resort. For a whole host of reasons, the path is complex and difficult to tread, and it is often very difficult to balance the risks appropriately.

And, in any event, the firm may not have as free a hand to decide this question as you might think.

As well as the reputational and practical issues raised above, firms in the financial sector considering paying a ransom will need to look to their regulatory responsibilities to prevent financial crime, the operation of sanctions regimes in various jurisdictions (particularly in the U.S.), the stance of their regulators on the issue, information held by cybersecurity organizations such as the U.K. National Cyber Security Centre, any law enforcement agencies that may be involved, and — importantly — the views of their cyber liability insurance carrier, which, depending on the severity of the incident, may not always be adverse to the idea of payment.

This is particularly the case where the ransomware incident is so severe that it prevents, or threatens to prevent, the firm from being able to operate at all. In such a do-or-die scenario, the desire on the part of the board of the affected company to make payment to save the firm is often overwhelming.

However, it's important to remember that the inputs to a decision as to whether to pay a ransom potentially come from far and wide, and will require balancing the views of multiple interested stakeholders.

As a result, before making any decision as to whether to pay a ransom, a business faced with a ransomware incident should focus first on business continuity, investigation and containment. It will need to move quickly to activate any business continuity plans, obtain legal advice, bring in security experts and engage early, but strategically, with key stakeholders.

The key to strategic engagement is knowledge — approaching stakeholders from the position of being able to articulate what the incident is, what risks it poses, what the implications are for the business and what recovery looks like, will be key to finding the right way through the maze.

In our experience, when dealing with stakeholders — particularly regulators — the temptation can be to circle the wagons; to hunker down until the immediate storm has passed. But in many cases this course of action risks making the situation worse in the long run: Failing to inform the financial regulators can have enforcement implications, and not involving the insurance carrier at the appropriate point risks invalidating the firm's cover. Strategic decision making on what, and when, to disclose is therefore one of the keys to a successful response.

U.K. Disclosure Requirements

In the EU, the unavailability of systems and data as a result of a cyberattack is likely to trigger notification requirements to the relevant privacy regulator because unauthorized access to personal data is a "personal data breach" within the meaning of the General Data Protection Regulation. For the U.K., this regulator is the Information Commissioner's Office, or ICO.

Notification to the ICO may prompt follow-up queries, and a proactive approach to managing the process of providing information to the ICO is vital. If individuals are likely to suffer harm as a result of the data breach, they too must be notified of the incident, the risk to them and the steps that the firm will take to mitigate that harm.

Furthermore, a ransomware attack is also potentially notifiable to the relevant financial services regulator. The Financial Conduct Authority, or FCA, generally expects to be notified under Principle 11 of material cyber events at regulated firms.

The regulator defines such an event as one that involves significant loss of data or control of IT systems; affects a large number of customers and could result in harm to them — this can include business customers, not just individual consumers; or results in unauthorized access to information and communication systems, or places malicious software on computer systems.

The FCA takes this position both because of the potential impact on consumers and the fact that the incident may indicate to the regulator that there is an issue concerning the efficacy of the firm's systems and controls, or its outsourcing arrangements.

The FCA handbook provides guidance on the application of Principle 11, and SUP 15.3 notes that the FCA would expect to be notified under Principle 11 of "any significant failure in the firm's systems or controls."

For dual regulated firms, the Prudential Regulation Authority, or PRA, has similar requirements to disclose, although it will generally be concerned about the impact on the prudential position of the firm and its systems and controls, more than the impact on customers in and of itself.

The key question is always what to disclose to the regulator and when to disclose it. In the financial sector, often a call to the firm's supervisor informing them of the incident and following up in writing will be sufficient to discharge the initial duty to notify.

Regulators understand that — particularly in ransomware incidents — firms may have imperfect information, and the supervisors will often be grateful to know earlier rather than later, even if this means they receive an incomplete report. Once a notification is made, however, it will be vital to provide regular updates as new information becomes available.

Payment — Regulatory and Other Implications

In the financial services context, other than noting that there are risks to paying the ransom and repeating the National Crime Agency's view that making payments is very risky, the FCA and PRA have not taken a firm stance against payment from a regulatory perspective.

The calculus, therefore, as to whether payment is a viable option in the financial services industry will involve weighing up the implications for the business and customers of refusing payment versus the costs of doing so. Often the cost of paying the ransom pales into insignificance compared to the overall cost of dealing with the incident itself, and this becomes more acute if the incident has effectively shut the business down.

It's here that the cyber insurer's view sometimes comes into sharper focus: They may be happy to approve a ransom payment to avoid a larger claim for an extended business interruption event further down the line.

However, the legal implications of paying the ransom still need careful consideration: How will the firm satisfy itself that it is not breaching economic sanctions by making payment to a sanctioned entity? If there are reasonable grounds to suspect that the funds will be used for terrorist purposes, then could paying a ransom be a criminal offense under the Terrorism Act of 2000?

There may also be jurisdictions in which the firm operates where ransom payments are illegal. For example, in early October 2020, the Office of Foreign Assets Control and the Financial Crimes Enforcement Network in the U.S. each released advisory documents that raised the specter of potential regulatory or enforcement action for making or facilitating certain ransomware payments.

FinCEN noted that the facilitation of ransomware payments may require intermediaries to register as money service businesses and make suspicious activity reports. OFAC noted that making ransomware payments to sanctioned individuals or entities could breach U.S. law.

While it is possible to analyze these questions, it's not always straightforward where the threat actors may appear effectively anonymous. However, it is here that engaging security experts, and having a

reasonably open line of communication with regulators and law enforcement can be helpful in allowing the firm to access sources of intelligence concerning the threat actors that might not otherwise be available.

International Issues

For firms that operate across borders, the risk of intervention by multiple regulators looms large, with all the complexities that such interventions bring with them. Experience suggests that in most cases where services are provided, cross-border regulators will be keen to understand the implications for the markets they regulate. As a result, a proactive strategy for dealing with regulators in all affected jurisdictions should be settled as part of the initial incident response.

The key issue will be to identify which regulators the firm proposes to notify proactively, and which will be left for later. Given that all regulators generally believe they should be the first to know, the judgments made here can be particularly fine. Simultaneous multiple notifications are unlikely to be realistic and, as a result, firms often accept that regulatory risks will arise in some jurisdictions.

Early analysis of business presence and impact of the incident in the affected jurisdictions is vital. From a strategic perspective, firms also need to consider competing regulatory requirements and to identify the jurisdictions most likely to give rise to risk of enforcement. The outputs of this analysis will drive the decision as to which authorities the firm decides to approach to make early, proactive disclosure.

Planning and Preparation

Handling a ransomware incident correctly is complex and inevitably requires a careful balancing of the risks to the firm's business against the risks to its reputation and regulatory status. In our experience, every incident response brings with it a highly charged atmosphere, with executives and board members under significant stress.

Ensuring that there is some form of corporate muscle-memory in place is vital to ensuring that the right decisions are taken in response to an incident, at the right time, with a clear and unified vision of the endgame.

Preparation for a ransomware attack is, therefore, vital. Each incident is different and will bring with it differing risks which will closely inform the strategy to be adopted in response. There are, however, a number of concrete steps that firms can take before an incident hits that will have a positive impact on preparedness, including:

- If you don't already have it, consider obtaining cyber and business interruption insurance.
- Speed is vital: Put in place a cybersecurity response team on retainer with expertise in responding to ransomware events.
- Establish your corporate policy for the firm's response to a ransomware payment request in consultation with your internal or external counsel and cyber insurance carrier, including establishing the legality of making a payment at all, and in particular the effect of doing so on your insurance cover.

- Produce an incident response playbook to establish who you would call in the event of a ransomware attack and ensure their contact information is up to date (law enforcement, external counsel, insurance carrier, regulators, incident response team).

- Review and refresh your incident response playbook frequently — working through relevant scenarios to establish the procedure and to identify any missing links or weaknesses is vital.

- Define particulars of when, how and under what conditions the decision to pay or not pay might be made. Executive "tabletop exercises," where the firm war-games a situation in which it is subject to a fictional ransomware incident, to which executives are required to respond, allow the firm to stress-test decisions that executives will need to take if the event occurs.

- If the payment of ransom is determined to be a potential option as a matter of policy, plan for how you would make the payment — including in bitcoin or other digital currency if needed. In addition, consider forming a relationship via your incident response team with a third party that you might use facilitate payment on your behalf. Your advisers, including external security teams and legal advisers, may have their preferences — as will your insurers, who may require use of a particular party.

Rob Dedman is a partner and Kim Roberts is counsel at King & Spalding LLP.