HERBERT SMITH FREEHILLS

FSR OUTLOOK 2022: RANSOMWARE - THE BAD GUYS ADAPT THEIR BUSINESS MODEL

07 December 2021
Legal Briefings

Explore our FSR Outlook 2022

Organised crime gangs have adapted their business model to target banks and other financial services firms

In a nutshell:
- **Ransomware attacks are big business and ransom demands have grown**
- **Firms should consider ransomware scenarios and whether a ransom could lawfully be paid**
- **Preparation is key!**

Just a few years ago, we would from time to time read about ransomware attacks in which millions of computers in dozens of countries had been compromised and, for a small payment, those affected could buy the key to unlock their laptops. Now it is more likely that an attacker will target a large corporate and spend weeks secretly roaming around servers; gathering confidential information to be used as a bargaining chip; accessing information about insurance cover to help set a tempting ransom demand and making sure that when an attack is launched it takes down not only the main servers but also any back-up. The amounts demanded as ransom have also increased but they are carefully pitched to make the payment of a ransom an attractive commercial proposition. Because the attacker has often taken down systems and also has data that a company wants returned or destroyed, the commercial calculation is not simply about recovery time and cost compared to the ransom demand.

So frequent are the attacks and so crippling the consequences that many financial services firms have moved from the policy stance: "We don't pay ransoms!" to the question: "Can we lawfully pay a ransom?" The answer to that question, and the hoops you need to jump through varies from jurisdiction to jurisdiction but in many jurisdictions the answer is a qualified yes – particularly if the threat actor is not on a sanctions list. And, curiously, because it's a business for organised crime gangs they want you to trust them. You can often have a good level of confidence that payment will get you what you bargained for: your systems up and running and your data returned.

Ransomware attacks can unfold with devastating speed. Wise firms have practised the scenario; considered their vulnerability to direct attack or attack via a third-party supplier; thought through the possible consequences for customers and counter-parties; understood the legal questions arising if a payment is made; reviewed their insurance cover and debated the policy issues.

There are dozens of time-critical questions that arise when you are under attack, including: Who are the attackers? What have they compromised? What do we have to tell markets or regulators? Which regulators and how long do we have? What do we know about the impact on customers or counter-parties? What should we say to reassure those customers and counter-parties? What might we be required to say? How can we even communicate with customers and counterparties when all our systems are down and we can't update our website? How can we communicate internally when our systems are down and may be compromised: are the criminals reading our emails? Can we legally pay a ransom? If the threat-actor is on a sanctions list, is it practical to get official permission to pay? Do any defences apply? What are the chances of prosecution if we pay anyway? Will the board be in the dock: could individual decision makers be prosecuted? If we decide to pay a ransom, how do we buy the virtual currency and who are our intermediaries? Does our insurance cover this?

The regulatory setting for all this is operational resilience. The effect of regulatory pronouncements on operational resilience in major jurisdictions is that financial services companies cannot be in denial. Companies must assume failure, for example because of a ransomware attack, and plan accordingly: they must identify their important business services or activities; set risk tolerances for the maximum time those services can be down and then devise strategies for staying within those tolerances. That now includes thinking through the ransomware scenario before you know you have been attacked. The criminals may already be inside your servers.

Cyber resilience standards and expectations for financial services and other organisations are already becoming more prescriptive and more complex, with a maze of intersecting regimes and reforms on the horizon. Regulators have sounded warnings that they will take action for failures to meet those standards. Action has already been taken in some jurisdictions.

And the answer to that question on how long you have to tell the regulators? In Singapore, you have a whole hour. In the EU, if a payment service is disrupted, once you have classified the incident as "major", you have four. In Australia, where the Reserve Bank has warned that a significant cyber security attack against one of the nation’s banks is all but “inevitable”, the expectations depend on the circumstances including the impact of the incident on the regulated entity: notification to various regulators may be required in 12, 24, 72 hours or “as soon as possible” - a complex matrix of obligations to navigate. In the UK, they don't bother to set a time: the FCA guidance is clear and notification is required "immediately" where the situation could have a significant adverse impact on the firm's reputation; or could affect the firm's ability to continue to provide adequate services to its customers; or could result in serious detriment to a customer. But in many cases, the decision on who to tell and when will be taken out of your hands. The attack will be taking place in the full glare of the 24-hour media.

As we go to press, we are seeing the first signs, especially in the USA, of whole-of-government efforts to disrupt the criminal gangs behind ransomware attacks. One crime boss responded: "Thanks, I'm off!" but we expect the fight to continue for years to come.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW PROCTER
CONSULTANT, LONDON
+44 20 7466 7560
Andrew.Procter@hsf.com

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

JOHN O'DONNELL
PARTNER, NEW YORK
+1 917 542 7809
John.ODonnell@hsf.com

CHRISTINE WONG
PARTNER, SYDNEY
+61 2 9225 5475
Christine.Wong@hsf.com

LEGAL NOTICE