Acuris Risk Intelligence

Nick Parfitt is head of Market Planning at Acuris Risk Intelligence. He can be contacted on +44 (0)203 741 1300 or by email: info@acuris.com.

SPOTLIGHT ARTICLE July 2020

The coronavirus pandemic, practical steps to safeguard the organisation and its employees

BY NICK PARFITT

The COVID-19 pandemic has shown how vulnerable the modern world is. The disease spread outside of Asia within two months, damaging many states, businesses and human lives, and a 'state of emergency' has been declared in most affected jurisdictions. In an instant, the world became a borderless and confined place. Globalisation, with its interdependencies, free movement and integration, created risks for communities that are thousands of miles apart.

What does this mean for financial organisations and their staff at the sharp end?

While obvious, it must be stated that COVID-19 is causing non-reversable disruptions in everyday life. Social distancing, lockdowns and work from home requirements are making it difficult for all companies to effectively deploy any due diligence compliance and training programmes.

Our observations are that there have been a range of business impacts to financial institutions following the forced work from home directives. From an organisational perspective, just having the ability to move potentially thousands of staff to home working is fraught with risk and costs. Are home networks secure enough, given the highly sensitive customer data? Can the plethora of legacy systems be easily accessed? Furthermore, any data breach poses a real risk of financial loss through fines or loss of reputation, customers and sales.

Comparatively, training programmes should be less of a challenge. The current climate represents an excellent opportunity for employees to take those courses. Companies can help staff think about their financial crime compliance careers and really explore areas they may not have thought about, such as trade finance and environmental crimes, or more exotic areas such as arts and antiquities, as well as those

all-important cyber security policies and procedures.

From an employee perspective, companies need to be flexible and realise that a typical eight-hour working day may be now around six hours or less, depending on each persons' personal situation. If you have children, you cannot simply ignore them during the working day.

Several other important issues have emerged during the crisis. For example, an increase in the number of suspected white-collar crimes has been predicted. To date, we have not seen any spikes in white-collar crime, but it remains an important issue. Companies must manage their white-collar risks going forward, which requires them to understand how and where they are likely to be vulnerable. They need to ensure that they revisit and scrutinise systems, controls and policies; although they have essentially engaged disaster recovery procedures, it is unlikely that any company planned them to be in place for such a protracted period of time.

In terms of the forms white-collar crime could take, we would expect to see typical invoice-type fraud, which can take on myriad forms, and possibly insider trading given that would-be criminals are away from the prying eyes of the office environment.

Businesses should also be aware that criminals and gangs are utilising the 'dark web' to specifically target employees who are less secure and more relaxed while working from home, and thus may be more susceptible to their approaches. Typically, this means that business email compromise (BEC) and phishing attacks, as well as sophisticated 'boiler room' typologies, are far more common and successful. At present, emails and calls regarding COVID-19 drugs or government assistance are highly prevalent. Paradoxically, people are far more trusting through fear and thus are more likely to click on links in emails or fall victim to social engineering attacks.

Of course, there are several preventative steps, as outlined below, that businesses can take to guard themselves against these risks and ensure compliance and due diligence in these turbulent times, particularly as criminals often look for the 'low hanging fruit'.

First, companies must double down on education and communication with staff around the risks posed to themselves and the organisation, and make any training specific to the company's operations and its risk profile. If a company's customer data is highly sensitive, the company must ensure that working from home is as IT secure as it would be from the office. Particular attention must be paid to encryption and password strength standards for the home router.

Second, companies must consider what operations are 'business critical' and thus what can be postponed until employees return to the office.

Third, companies must have each employee risk assess their home circumstances for potential espionage or fraud and 'joint venture' collusion. For example, if employees have individuals who work for competing organisations sharing dwellings, this could be a potential 'red flag'.

Finally, do companies know what credentials and personal information on their business and employees is available for criminals on the 'dark web'? If not, then they should use this time as a wake-up call to find out.

Regarding criminality, and the environment that is now being created to allow this threat to expand rapidly, many companies' attitude to risk will have been sharpened by the pandemic and traditional models will need to be redesigned.

The biggest single risk to the global financial sector over the last 30 years has been its movement from a traditional and risk averse paper-based industry to a fast-paced digital ecosystem that drives risk against reward. The big bang in the 1980s was the catalyst for this, and the dangers exposed to us all in a brutal way during the global financial crash in 2008.

This cultural change was driven by the emergence and evolution of the internet and the ability to trade in real time on global stock markets. The emergence of streaming technology meant that financial data could be exchanged instantaneously.

This new technology and the risks it presented gave vast, unheard-of profits to financial institutions, shareholders and governments, which all shared the spoils.

Why is this an important lesson from the past? The speed of change and relaxation of rules without any thought to risk and contingency allows bad things to happen. While the banking sector now has stringent regulations with margins and tight reserve targets to keep, this latest global disaster is perhaps where the banking sector repays some of its debt to the governments and taxpayers that bailed it out. With debt in the trillions now flooding the world, expertise in creating long-term bonds to lessen the immediate pain and help guide us back to economic growth will be a key solution.

Unfortunately, there is one group who will make billions from this disaster: criminals. The lockdown of services has diverted the attention of police and the increased vulnerability of citizens opens the doors for fraud and violations of all kinds. Criminals prey on vulnerable individuals and exploit their fears by offering fake goods and sending emails infected with malicious software, not to mention the complex money laundering and terrorism financing operations that are so difficult to detect, even outside of force majeure circumstances. Therefore, financial regulators and law enforcement agencies must operate as best they can in their 'business as usual mode' to defeat criminals. On 22 March, the US Department of Justice (DOJ) issued its first enforcement action against a fraudulent website which offered World Health Organisation (WHO) COVID-19 vaccine kits, which do not exist. US authorities have gone further by saying that coronavirus-related crimes can be charged as acts of terrorism.

Human kindness and naivety are often exploited by criminals. The theft of sensitive information using phishing and spoof emails and texts has increased significantly during this pandemic with bogus charity websites and credit card fraud promising medical potions and cures, huge discounts on designer goods or simply

the promise of riches. Someone always pays and someone always benefits.

It is the debt that you cannot see, crystallise or package as a bond that may have the greatest personal impact following this pandemic. The need for organisations and governments to educate their employees and customers on the pitfalls of cyber crime is a fundamental responsibility and one which banks seem reluctant to adopt. Currently, financial institutions seek to reimburse customers when cyber crime or hacking has taken place and when the transaction is genuinely agreed by the customer, either by giving a credit card number or sending funds. But who is responsible if the recipient is a fraudster? Why should a bank refund a customer if they have been careless?

During this pandemic and the economic crisis that will likely follow, billions will be lost to online fraud. Expect some nation states to sponsor sophisticated criminal activity to help save their economies, as well as the usual organised crime gangs.

To best protect themselves, companies must advise their staff and customers of several steps they can take during these perilous times. First, never click on a link in a text or email that looks suspicious. This includes offers of free cash such as prize wins, tax rebates, signing up for special offers or opening attachments and pictures from unknown senders. Second, report anything that does not feel right. Instinct is a valuable gift and is often right. Third, offer a 'darkweb' search capability to your staff to reassure them that their data is not being traded by criminals. Finally, avoid memory or USB sticks where possible, even if they are encrypted.

Regarding cyber security, it is worth considering that had the coronavirus been a computer bug the world would possibly find itself in an even worse position. The contagion would be instantaneous and only closed systems might survive. In real terms, this could mean no electricity, no mobile phones, no traffic lights, no heating, no payment systems and, of course, no internet.

For the financial sector, this would be far more serious, and it is worth asking regulators and governments alike what plans they have in place for such an occurrence. ■