CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 13

Wider lessons from Bangladesh

It's not just about the routers; the theft of USD 81 million from Bangladesh's central bank was widely blamed on poor security. The lack of a firewall and use of second-hand equipment turns out to be only half the story though, and there are implications for others who are much better prepared.

For a start, it's worth noting that it may have been Bangladesh's money, but it was transferred from the bank's account with the US Federal Reserve (fed). Bangladesh officials have insisted the fed shares the blame. The fed denies this, and there have been reports of potential inside help in Bangladesh Bank. If nothing else, it's a reminder that security is only as good as the weakest link.

It's also sobering that the theft – already among the biggest bank raids in history – could have been much worse: The hackers attempted to steal close to USD 1 billion and were only prevented from doing so – according to reports – by a typo and an alert correspondent bank.

The most worrying aspect for businesses, however, is reports of potential weakness in the Society for Worldwide Interbank Financial Telecommunications (SWIFT) payment system itself. The system is the main method used for secure international interbank messages, which include financial information.

As one commentator told the *Financial Times*: "Central banks have been looking at cyber crime, first at their banking sector and more recently with regard to their own websites. But real-time gross settlement systems and SWIFT are in a different league. You are not just talking about big money, but the money; SWIFT is the nervous system of international payments."

◀◀ *Continued from page 1*

WIDER VULNERABILITIES

Again, suggestions in Bangladesh that SWIFT shared the blame have been flatly denied. All three – Bangladesh Bank, SWIFT and the Federal Reserve – now seem to have come to an uneasy truce.

However, security consultant BAE Systems did identify sophisticated malware used in the Bangladesh attacks. Moreover, while SWIFT has said this had no impact on its network or core messaging services, it has since confirmed the Bangladesh attack was not an isolated incident.

"The malware used in the earlier reported customer incident was not a single occurrence, but part of a wider and highly adaptive campaign targeting banks," it states.

Reports suggest the second attack using the malware was on an unnamed commercial bank in Vietnam. SWIFT has urged all customers to "review controls in their payments environments."

> "Crime policies, meanwhile, are set up to cover illicit funds transfers and theft, but may contain exclusions for cyber events"

ANOTHER HOLE

There's one final aspect that has been less mentioned, however, which is that banks and others may need to fill another significant hole in their protection: insurance.

It's generally assumed thefts such as these will – since they involve computers – be covered under a cyber policy. Others, meanwhile, assume they have cover under their crime policy. In fact, there's no guarantee either will pick up such losses.

While there's an increasing variety, most cyber policies are still focussed on traditional data breaches, providing cover to combat and remedy losses of personal information. They are not generally designed to cover financial crime. Crime policies, meanwhile, are set up to cover illicit funds transfers and theft, but may contain exclusions for cyber events, whether social engineering attacks, such as phishing, or straightforward hacking. It is worth speaking to your broker about ways you can ensure seamless protection through innovative solutions.

Either way, the SWIFT attacks are a reminder to everyone to not just review their defences and controls, but also examine their insurance wordings for any gaps in cover. ■

Good news and bad news for cyber claims in general insurances

The recent decision in the Portal Healthcare case in the US has potentially brought more coverage, but less certainty for businesses there. Longer-term it might also have consequences for insurance of data breaches over in Europe.

The decision challenges insurers' argument – routinely applied – that the cover provided by commercial general liability (CGL) policies for "publication" of material violating privacy is not intended to apply to data breaches.

In the Portal Healthcare case, medical records and notes of 2,000 hospital patients were potentially exposed during a data breach in 2013, prompting a class action. The insurer refused to pay for the costs of defending the claim; it argued the hospital did not intended to release the information and there was no evidence anyone had seen it, so that no publication had taken place.

The court disagreed. Publication took place regardless, once the information became accessible to unauthorised third parties via the internet. The decision is significant.

"It opens new avenues of coverage for companies forced to litigate class actions alleging disclosure of private data in a cyber attack," notes one US legal firm.

MORE EXCLUSIONS AHEAD?

Despite this, US businesses should not get too excited.

First, as others have noted, the court did not rule the insurer must pay for any damages if it loses the case – only that it should pay for the insured's defence. Second, at the state level, others still expect there will be cases that go against insureds.

Most significantly, the case is expected to only accelerate moves from some insurers to seek explicit exclusions of data breaches in their general liability policies. Indeed, the same lawyer heralding the new avenues of coverage also predicts cyber insurance "will become increasingly important as new exclusions are added that limit CGL coverage."

In Europe, meanwhile, insurers still generally accept cover for such breaches, so the issue does not arise. With the possibility of class actions for data breaches only just emerging in the UK and increased requirements from the General Data Protection Regulation (see next page), however, that might not last forever.

As the risks increase, it may not be too long before general liability insurers here look to their US colleagues for ideas about how to limit their exposure. ■

The countdown begins: The EU Data Protection Regulation

After four years of consideration the European Parliament has finally passed the General Data Protection Regulation (GDPR). The regulation, the final text of which is now available, will apply automatically across the EU – without requiring new national laws to implement it – from 25 May 2018.

The headline provisions – such as fines of up to four per cent of global turnover or EUR 20 million for breaches – have been known for some time. Businesses also still have two years to prepare. However, many have their work cut out.

For a start, some changes are likely to be felt well before 2018. One result of the passing of the regulation will be increased attention on data privacy rights: the European Commission is promising public awareness campaigns to publicise the new rules.

> "Some insurers will offer additional retroactive coverage, and for many insureds this is well worth any additional premium spend"

If businesses have not already started to prepare, they also face a significant exercise: They will need to review data protection policies; check their technological defences (including encryption); and map out their data exchanges within their organisation and with third parties to examine their vulnerabilities. The regulation is likely to make data protection a board-level issue, says security firm Sophos.

A big part of the exercise must also be to revisit the requirements for cyber insurance.

The introduction of mandatory notification of individuals when their data is breached drove the market for cyber insurance in the US; it's long been expected introduction of the same in Europe under the GDPR will have a similar effect here.

If businesses are considering cyber inusrance, they need to start now. First, because assessing needs and buying cyber insurance for the first time can be quite an involved process, and with board level attention risk managers will want to make sure they have done appropriate due diligence on the new cover. Second, because most new cyber insurance policies are offered on a retro-inception basis, businesses will only be covered for notification costs of data breaches occurring after cover is in place. Breaches that began before – even if they are only subsequently discovered – will not typically be covered. Some insurers will offer additional retroactive coverage, and for many insureds this is well worth any additional premium spend.

Given the long latency period of many breaches in past, it is feasible that vulnerabilities exploited by hackers in the coming year will only be identified after the new regulation is in place. If businesses want to be sure of protection against notification and other costs under the new regime, then, time is already running out. ■

"Given the long latency period of many breaches in past, it is feasible that vulnerabilities exploited by hackers in the coming year will only be identified after the new regulation is in place."

What's floating your boat

The Internet of Things (IoT) is vastly expanding the range of possible exposures into new areas, such as shipping.

Allianz's annual Safety and Shipping Review shows generally positive trends for losses in the shipping industry: Large shipping losses have declined by 45 per cent over the last decade. One area of increasing concern, however, is the cyber risk the industry faces.

"The maritime industry's reliance on interconnected systems poses risks as well as bringing benefits. Threats can result from improper integration and interaction of cyber systems/updates or attacks from external sources and are not always detected," the report notes.

It is not the first to note the risk: Verizon's Data Breach Digest report details a shipping company targeted by pirates who were hacking into its sever to access details of inventories and bills of lading. The information was then used by the pirates to target particular vessels and particular storage containers once on board.

Longer-term, the cyber risk won't be restricted to business systems either. Allianz cites a paper by the Lloyd's Market Association to argue that IoT and reliance on e-navigation may see hull or machinery damage resulting directly from cyber attacks within five years. Already, the report cites the case of a hacker causing an oil platform off the coast of Africa to tilt to one side, forcing a temporary shut down.

"The maritime industry's reliance on interconnected systems poses risks as well as bringing benefits. Threats can result from improper integration and interaction of cyber systems/updates or attacks from external sources and are not always detected."

We've detailed before how the possibilities of the IoT also bring risks. Businesses in the shipping industry, as elsewhere, therefore need to consider the likelihood of property damage or loss of goods from a cyber event, particularly since many cargo policies will include a version of the CL380 Cyber Attack exclusion, and while the newest version is modified to give back physical damage cover, underwriters have stated that their intent is still that and "systemic" cyber issues are not covered. As ever, insureds should start with a gap analysis, considering the potential risks and their current cover under existing policies. ■

45%

Large shipping losses have declined by 45 per cent over the last decade, but cyber is an increasing concern.

BUZZWORD OF THE MONTH

PCI DSS

What is it?

The payment card industry data security standard (PCI DSS) is a security standard for all those handling credit cards from the major card companies such as Visa, MasterCard and American Express. An updated version – v3.2 – was published in April.

Administered by the PCI Security Standards Council its intention is to increase data security and reduce internet-enabled payment card fraud. There are 12 headline requirements, such as a requirement to install a firewall to protect cardholder data and encrypt cardholder data transmitted across public networks, for example. Underneath each, however, are a large number of more detailed obligations that elaborate how the requirement can be met.

These are all designed to enable those following the standard to meet six objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy.

Why should you care?

Because, as the PCI SSC notes, "If you are a merchant of any size accepting credit cards, you must be in compliance with PCI Security Council standards." They also apply to any other organisation that accepts, stores, transmits or processes cardholder data.

The new version of the standards includes a number of changes, including requirements for multi-factor authentication for administrators accessing cardholder data and additional extra security validation steps for service providers. One central change is clarification of the need to ensure data security controls are always in place and effectively tested under an on-going security monitoring process, meaning that technology alone will not meet the required standard, and processes will need to be strengthened.

The old version of the standard will be retired in October and all firms will then be assessed and audited against v3.2. The PCI SSC are urging firms to adopt the new standard as soon as possible, however.

Remember as well that if you are a payment card accepting merchant, your merchant services agreement will typically pass on liability to you for PCI assessments. These can include fines for non-compliance with the security standard, operational expense recovery amounts, and also fraud recovery amounts. While many retailers have asserted that these amounts are arbitrary and even unlawful, they can still be quite costly even when negotiated. These assessments have recently been the topic of cyber insurance coverage litigiation, so it's more important than ever to carefully review the scope and the amount of any coverage you currently purchase for all things PCI-DSS. ■

Cyber threat intelligence

Brought to you in partnership with CSC

THINK YOU UNDERSTAND THE DARK WEB? THINK AGAIN

Much of the cybercrime threat landscape is associated with the dark web, and there's no shortage of news on its dangers. As the *Decoder* has covered before, however, it's not always well understood. That limits the ability to assess the threats and make informed decisions about how to deal with them.

For a start, the terms "dark net", "deep web" or "dark web" are often misused, giving the impression of a single organised technology platform requiring technical expertise to access.

In fact, the deep web is not that different from the normal web we all know: The sites available from Google, Bing,Yahoo or other mainstream search engines. It is still publicly accessible but is just generally overlooked by the indexing attempts of search engines due to restrictions on their crawlers, password protected forums, paywalls or similar barriers.

The dark net, by contrast, is truly invisible to the public network. It include corporate intranets, home servers, as well as sites using hidden networking technologies. It's just the last of these most people are talking about when they discuss the dangers of the dark net, though.

Even here, is not a single entity: the most common hidden network technology is Tor, which wraps messages sent by users in layers of encryption and bounces them between network nodes before sending them to a destination either on the internet, or a site embedded within Tor (known as an onion site and not accessible from the internet). However, the dark net also includes a number of other technologies: I2P (the invisible internet project) and Freenet make up the top three. All have legitimate – as well as illegal – uses.

This again illustrates the futility of those who'd like to see the dark net "shut down". It can't be shut down; the risks it raises can only be managed. And a good start, is to ensure it is understood.

RECENT VULNERABILITIES AND THREATS

May 23 LinkedIn has completed its invalidation of passwords for all accounts created prior to 2012, according to a statement from the company. It follows attempts on the dark web to sell 117 million users' emails and passwords resulting from a breach that year.

May 13-18 Hackers affiliated to the anonymous group attacked 18 banks and financial institutions in a week with distributed denial of service (DDoS) attacks, as part of its "Oplcarus" campaign. Targets have included the New York stock exchange, Bank of Scotland, Bank of France, five US Federal reserve branches, and the Bank of England.

May 16 Kaspersky is warning that the Olympic Games in Rio de Janeiro are the focus of continued criminal activity, with scam emails and fake ticketing services using counterfeit websites employed to target victims. Emails usually contain very brief text and attachments (typically in PDF or DOC format) to lure the user into thinking they have won a competition for free tickets.

May 12 Telecom company TalkTalk's profits have more than halved following the cyber attack on its systems last October, according to the company's preliminary results. The fall, to £14 million compared to £32 million a year ago, is at least partly due to the £42 million costs of the attack, which saw the personal data of nearly 160,000 people accessed. ■

JLT Specialty Limited provides insurance broking, risk management and claims consulting services to large and international companies. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust – often unique – solutions. We build partner teams to work side-by-side with you, our network and the market to deliver responses which are carefully considered from all angles.

Our Cyber, Technology, and Media Errors & Omissions team delivers bespoke risk management and insurance solutions to meet the needs of clients from a variety of industries. The team combines experience and talent with a track record of delivering successful results and tangible value for our clients.

CONTACTS

Sarah Stephens
Head of Cyber,
Technology and Media E&O JLT Specialty
+44 (0) 20 7558 3548
sarah_stephens@jltgroup.com

Lauren Cisco
Partner, JLT Specialty
+44 (0) 20 7558 3519
lauren_cisco@jltgroup.com

Jack Lyons
Partner, JLT Specialty
+44 (0) 20 7528 4114
jack_lyons@jltgroup.com

JLT Specialty Limited
The St Botolph Building
138 Houndsditch
London EC3A 7AW
www.jltspecialty.com

Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority. A member of the Jardine Lloyd Thompson Group. Registered Office: The St Botolph Building, 138 Houndsditch, London EC3A 7AW. Registered in England No. 01536540. VAT No. 244 2321 96.

TOP TWEETS

The latest from JLT on terrorism, including our view on cyber terrorism

50 million exposed in Turkey data breach

5 things to look out for in a cloud service provider

Time to face up to cyber risks

@sarahmstep nominated for Cyber Risk Industry Person of the Year

Cyber-insurance 'vital', but businesses aren't taking it