REPRINT

R&C risk & compliance

CYBER AND RANSOMWARE RISKS FACING FINANCIAL INSTITUTIONS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
OCT-DEC 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Acuris Risk Intelligence

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com
© 2019 Financier Worldwide Ltd. All rights reserved.

www.riskandcompliancemagazine.com

MINI-ROUNDTABLE

CYBER AND RANSOMWARE RISKS FACING FINANCIAL INSTITUTIONS

PANEL EXPERTS

Nick Parfitt
Head of Market Planning
Acuris Risk Intelligence
T: +44 (0)20 3741 1200
E: info@acuris.com

Nick Parfitt is responsible for determining Acuris Risk Intelligence's approach to the market and building subject-matter expertise. He has 18 years' experience in project and programme management, business process change and in implementing technology and business solutions at financial services, telecoms and public sector organisations. His experience in the financial crime sector spans seven years helping tier 1 financial institutions assess and improve AML, KYC and sanctions operations. Mr Parfitt has worked for several tier 1 banks in the UK and holds an MBA (Distinction) from Cardiff University, and a BA (Hons) in Biochemistry from Imperial College.

Rebecca Hughes Parker
Global Editor in Chief
Cybersecurity Law Report

Rebecca Hughes Parker is an attorney and global editor-in-chief of the Cybersecurity Law Report and the Anti-Corruption Report, managing a team of lawyers and journalists. She also writes and edits extensively, moderates panels and speaks publicly as an expert on anti-corruption compliance, cyber security and data privacy law. Previously, she was a litigator at Dentons, where she represented clients across a range of legal areas, amassing significant trial, appellate and internal investigation experience and earning the firm's pro bono prize. Earlier in her career, she was an award-winning broadcast journalist at metro-NYC stations.

R&C: How would you describe the extent of the cyber threat currently facing financial institutions (FIs)? Are you seeing an increase in ransomware attacks?

Parfitt: The July 2019 Capital One breach made it very clear, if it was not already, that the financial industry is not safe from large-scale attacks. This breach originated via a cloud vendor, but the many threats facing the financial sector continue to increase. Ransomware in particular has evolved into 'malware disguised as ransomware' – a ransomware attack that can now destroy, exfiltrate or encrypt data. We saw this with the NotPetya attack in 2017. Other threats include DDoS attacks, social media attacks, spear phishing, PoS malware, ATM malware and credential theft. The increased use of biometrics also poses new security threats, as does quantum computing. There continue to be threats stemming from employee error or carelessness. When employees use public Wi-Fi or a deficient private network, they can also open the FI up to hackers, as they do, of course, when they click on a spear phishing email. Business email compromise in particular was the subject of a recent US Securities and Exchange Commission (SEC) warning. Nine public companies that fell victim to these scams lost a total of nearly $100m to the perpetrators. The SEC noted that these scams were successful "at least in part, because the responsible personnel did not sufficiently understand the company's existing controls or did not recognise indications in the emailed instructions that those communications lacked reliability".

R&C: Generally speaking, how aware are FIs of the range of potential cyber attacks they face? Is the issue of cyber security firmly on the agenda for boards and C-suite executives?

Hughes: Cyber security and data privacy is the agenda on the board of more FIs than ever before – and certainly should be if it is not. We are told that the recent high-profile cases of Equifax, Uber, Marriott, British Airways and now Facebook have raised the profile of both data security and privacy at board level. The SEC issued guidance in February 2018 around cyber-related disclosures and governance and that also played a role in elevating the issue. When it comes to privacy, Facebook's settlement with the US Federal Trade Commission (FTC) also places a strong emphasis on accountability from the top. The settlement mandates the creation of an independent privacy committee comprised of independent directors who meet certain privacy and compliance requirements – these are requirements we have not seen before in these kinds of settlements. FIs can examine this model and decide whether it will work for them in terms of both privacy and security.

R&C: What steps should FIs take to defend against attacks?

Parfitt: Designating a chief information security officer (CISO) is a wise option. It is often better to have a CISO develop the programme than tasking a chief technology officer (CTO) or chief information officer (CIO) with it. Companies should take steps to ensure that cyber security is an enterprise-wide risk and not just an IT risk. We often hear that there is a communication gap between information security and information technology on one hand and legal and compliance on the other – these teams need to work together and bridge that gap with clear lines of communication and no assumptions that each team understands all the terms. Apart from governance, important components of a security programme include conducting regular risk assessments and implementing effective processes that address access rights and controls, data-loss prevention, vendor management, training and incident response.

R&C: What role do technologies such as artificial intelligence (AI), machine learning (ML) and data analytics have to play?

Hughes: AI, ML and data analytics can all play an important role in security. For example, AI and behavioural-based anti-malware software looks for file and operating system changes that are out of line with normal computer operation – this can also work for mobile phones and tablets, which are attractive entry points for hackers. Companies should be aware of the various regulations that govern the use of these methods, such as the General Data Protection Regulation (GDPR). AI is subject to each of Article 5 of the GDPR's general principles for processing data and Article 22 addresses decisions based on automated processing, for example.

> **"FIs need to know where their data is – and our conversations reveal that they increasingly understand that data-mapping is an important first step."**
>
> *Nick Parfitt, Acuris Risk Intelligence*

R&C: With the uptick in cyber security threats leading to more stringent regulations, such as the General Data Protection Regulation (GDPR), how

are FIs coping with rising compliance requirements? What solutions are available to help FIs manage the costs and complexities involved?

Parfitt: FIs need to know where their data is – and our conversations reveal that they increasingly understand that data-mapping is an important first step. An updated and compliant privacy notice is also foundational. If an FI must comply with the US's Gramm-Leach-Bliley Act, it has published a privacy notice, but revisiting that and ensuring transparency is important, especially for FIs subject to the GDPR. For GDPR compliance, other crucial steps include reviewing third-party contracts – some companies have told us that to get a handle on their third parties, they had to look at a list of accounts payable – assessing whether a data protection officer (DPO) is needed, and identifying the bases for processing data. Also important is developing a procedure for answering data subject requests and making sure that the company properly preserves its defences for the legal bases of data uses under GDPR Article 6.

R&C: What advice would you offer to FIs on constructing effective frameworks, policies and processes to address cyber security vulnerabilities, including ransomware defence?

> **"Backups can be lifesavers in ransomware attacks, as can segmenting data so that the attack can be contained."**
>
> *Rebecca Hughes Parker, Cybersecurity Law Report*

Hughes: Updating and patching are key. Many companies, such as Equifax, have got into trouble because they did not implement a known update. Backups can be lifesavers in ransomware attacks, as can segmenting data so that the attack can be contained. Being part of an information-sharing group can also help the FI quickly determine more about the type and severity of the attack. R&C