

Preparing for an IT Audit

2020

1. Strange Times
2. Operational Resilience
3. Steps to take
4. Other Issues
5. The future



Simon Whittaker

The majority of my work involves working with companies to perform penetration & security testing, test and improve secure coding practices and provide security consultancy to companies that are keen to improve their processes & procedures

`simon.whittaker@fscom.co.uk`

1 Strange Times

‘Disruptive events can have a high impact on consumers and businesses so firms and FMIs need to know where the risks to their service delivery lie and to make sure that they are prepared for any service disruption by testing their planned response.’

Andrew Bailey, FCA Chief Executive

Offices –
remember them?





The New World

Over the coming months, everyday life will be disrupted in ways that will cause severe financial difficulties for many thousands of businesses, families, and individuals.

- Our main priorities are
 - To ensure that financial services businesses give people the support they need
 - That people don't fall for scams
 - Financial services businesses and markets know what we expect of them.

Our proposals make it clear that we expect firms and Financial Market Infrastructures (FMIs) to take ownership of their operational resilience and to prioritise plans and investments based on their public interest impact.

<https://www.fca.org.uk/publication/consultation/cp19-32.pdf>

Travelex forked out multi-million ransom to restore its systems

By Anthony Spadafora 25 days ago

Millions paid out to cybercriminals

New York payments startup exposed millions of credit card numbers

Zack Whittaker @zackwhittaker / 10:36 pm BST • April 22, 2020

Comment



Image Credits: Damien Meyer / Getty Images

A massive database storing millions of credit card transactions has been secured after spending close to three weeks exposed publicly to the internet.

paid a
encrypted.

THE WALL STREET JOURNAL.

English Edition | May 5, 2020 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

PRO CYBER NEWS

SEC Urges Better Cybersecurity Practices at Financial Firms

Regulator details strong safeguards it has observed at companies it oversees



A person fa
the approac
PHOTO: AND

Exchange rate service's customer details hacked via AWS

20 MAR 2020 0

Data loss, Security threats



Previous: COVID-19 disruption delays release of Chrom... Next: Trolls ZoomBomb work-from-home videocall with...

by Danny Bradbury



Online exchange rate data provider [Open Exchange Rates](#) has exposed an undisclosed amount of user data via an Amazon database, according to a notification letter published on Twitter this week.

MOST POPU

1. Kim Jon
Emerge:
Smoking
2. Cruise S
as Coror
3. Coronav
Lockdov
Expire, I
Investig
4. As Ferra
Staff Art
Coronav
Tests
5. What Cl
Tells Us
Coronav
Econom

MOST POPU

1. The Seci
Scientis
Billionai
Manhatt
Covid-15
2. Should \

2 **Operational Resilience**

Building operational resilience: impact tolerances for important business services

- Identify their important business services that if disrupted could cause harm to consumers or market integrity, threaten the viability of firms or cause instability in the financial system
- Set impact tolerances for each important business service, which would quantify the maximum tolerable level of disruption they would tolerate
- Identify and document the people, processes, technology, facilities and information that support their important business services
- Take actions to be able to remain within their impact tolerances through a range of severe but plausible disruption scenarios

Press Releases Published: 05/12/2019

Last updated: **31/03/2020**

<https://www.fca.org.uk/news/press-releases/building-operational-resilience-impact-tolerances-important-business-services>

3 Steps to take

What services are important?

identify their important business services that if disrupted could cause harm to consumers or market integrity, threaten the viability of firms or cause instability in the financial system

What is your tolerance for failure?

Set impact tolerances for each important business service, which would quantify the maximum tolerable level of disruption they would tolerate

People, processes & tech

Identify and document the people, processes, technology, facilities and information that support their important business services

Actions to keep going

Take actions to be able to remain within their impact tolerances through a range of severe but plausible disruption scenarios

EBA Guidelines for Cyber Security

- Information Security Policy
- Logical Security
- Physical Security
- ICT Operations Security
- Information Security reviews and testing
- Information Security training and awareness



4 Other Issues

Staff

“Relying on developing an effective technical control environment alone may not deliver the best results. It needs to be accompanied by positive steps to increase staff awareness and understanding, such as providing training and engaging with high-risk personnel.”



Suppliers

FCA have said that 17% of the incidents firms reported to them were caused by IT failure at a third-party supplier – the second highest root cause of disruption to services





5 The future



Documentation & Risk

- You can't outsource risk
- Ownership – not just signing off
- Practical Measures
- Suppliers
- Ask questions & **challenge**





Questions?