The Digital Operational Resilience Act (DORA) - bigger, better, faster, stronger

by Rois Ni Thuama

In 2004, at the Washington, D.C., headquarters of the Federal Bureau of Investigations (FBI), Chris Swecker, an assistant director, convened a press conference. Swecker was trying to highlight the problem of mortgage fraud, a problem he said, "has the potential to be an epidemic."

With little movement from the financial sector or regulators to address this known 'pervasive problem" that was "on the rise", Swecker held another news conference the following year in December 2005. This time he was joined by officials from the United States Department of Housing and Urban Development and the Internal Revenue Service.

The message was clear. The FBI had insight into a significant threat, which if left unaddressed, could create wholesale financial disruption and lasting economic damage. This was not a case of a crisis that was unavoidable, it is the case of weak corporate governance and weak risk management.

Why, you might ask, are we revisiting the causes of the financial crisis?

Credible sources and known threats

There are two good reasons for this. Firstly, any warning from the FBI should resonate with firms and be acted upon without delay. This is risk management 101. That is not a strange or unusual suggestion, that is elementary.

Yet despite repeated warnings from the FBI about significant cyber threats, businesses generally have been slow to address the most significant cyber threat.

The FBI's reporting unit IC3 reviewed data otherwise unavailable to the private sector and published their findings in the Internet Crime Report 2020. The FBI made the determination that Business Email Compromise (BEC) remains the most significant cyber threat by victim loss. Any reasonable director, legally obliged to exercise reasonable care, skill and diligence would of course address known significant cyber threats.

The FBI are not alone in issuing a stark warning about BEC. In the United Kingdom, the National Cyber Security Centre have warned that BEC (also referred to as phishing, CEO fraud, Friday afternoon fraud, invoice fraud and so on) represents the most significant cyber threat. So concerned are they that they have also issued guidance which includes deploying the global industry standard protocol (DMARC) as layer 1 defence.

This brings us to the second good reason why we must keep in mind the causes of the financial crisis. While the reform that followed the 2008 financial crisis strengthened the financial resilience of the EU financial sector, it broadly omitted Information and Communication Technology (ICT) risks.

The Digital Operational Resilience Act

To remedy this the EU has proposed a package of sensible measures aimed at the financial sector. This includes the Digital Operational Resilience Act (DORA) which is on the horizon due to become law as early as September 2021.

It will mean that financial entities must address:

any reasonably identifiable circumstance in relation to the use of network and information systems, - including a... misuse...or other type of malicious ...event - which if materialised, may compromise the security of the network and information systems.

What is meant by 'reasonably identifiable' would ultimately be a matter for the competent authorities and/ or the courts to decide. It is entirely conceivable that both bodies will take the view that information from credible sources, trusted, independent experts at the FBI and the NCSC ought to be considered as part of any sensible risk management strategy.

Certainly, no sensible counter argument could be made to suggest that the view from the Intelligence Communities (IC) ought to be ignored or omitted from consideration. That said, all firms would do well to review IC insights and address known threats, cyber or otherwise without delay.

The scope of DORA is sufficiently wide so as to capture a comprehensive list of every conceivable type of financial entity from banks to statutory auditors as well as applying to ICT third-party service providers. By making sure the scope is sufficiently wide, it means that not only will it benefit those firms that comply but that the broader financial sector will benefit as each firm plays its part in the ecosystem.

Here's an example to demonstrate this point: an investment firm that has taken the trouble to address any reasonably identifiable circumstance, will, in all likelihood, identify banks that have taken the same steps. It is unlikely that a firm that has gone to the expense and trouble of identifying digital risks would then tolerate a lower standard from its own suppliers. This strengthens the sector as a whole creating a virtuous cycle. The bottom line for investors and

protected and society benefits from the increased trust in the sector.

But the benefits mount up. DORA is a smart and necessary piece of legislation that will make the financial sector and the individual firms bigger, better, faster and stronger. This makes more sense if we start with better.

Better

Under DORA the management body of the financial entity must define, approve, oversee and be accountable for all arrangements relating to ICT risks. Moreover, the management body shall bear the final responsibility for managing the ICT risks. AND, they must be duly informed, needing to follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess cyber risks and their impact on the operations of the firm.

Having a better-informed management body that has skin in the game who are obliged to take part AND are no longer permitted to turn a blind eye can only serve to promote the success of the company (a statutory obligation) through better decision making to prevent unnecessary losses while simultaneously aligning with the directors' fiduciary duty to exercise reasonable care, skill and diligence, (another statutory obligation).

Mark Evans, Managing Partner with Define: Athene, who works with boards to build their cyber knowledge, explained that boards and management continue to improve firm value through wealth generation that is easy to measure. The problem, he explained, is that value preservation needs to be addressed via some fundamental cybersecurity measures, tools and policies.

Faster

Frequently the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO) will understand the cyber threat and the tool that they need to address that problem. Internally, they will champion for the speedy implementation of this tool, so far so good.

The problem often comes in the surprising form of the budget committee. While budget committees are a tested corporate governance tool providing extra eyes on spending, they are sometimes composed of people who understand neither the problem nor the solution. Instead of facilitating the purchase of an essential tool to protect the firm, they can act like sand in the wheels delaying, or even worse, scuppering, the purchase of important tools to defend the firm.

Anecdotally, there is plenty of cause for alarm as budget committees have vetoed cyber tools and solutions essential to protect the firm, only for the firm to be hit with a cyber-attack that was entirely avoidable. All it would take for a successful shareholder class action would be a single whistle-blower to come forward. Making faster decisions about important tools is critical to defend the corporation.

Faster decisions will be possible because the CISO or CIO within financial entities can now reference this piece of legislation (DORA) answering the questions which follow:

1. Is the threat a reasonably identifiable circumstance? In other words, is the problem well known and understood?
2. Is the source credible? There is considerable value in relying on trusted, independent experts such as the National Cyber Security Centre (NCSC) or the FBI for insight into cyber threats. Vendors frequently refer to themselves as experts, some are, and some are not. But none of them are independent. They have a clear business purpose, to sell their solution, so caveat emptor. Double check the problem exists before your business pays to solve it.
3. Is the solution a global standard protocol (or similar)? The tools to address the cyber threat should be proportionate to meet the threat.
4. Do reasonable IT directors recommend the solutions implementation or have governments or vendor neutral agencies, such as the NCSC, the US Department of Defence, NIST recommended the solution be deployed?

Answering yes to these four questions means that there is no reasonable excuse to delay. It means that better decisions can be made quickly and with certainty saving the firm time, money and additional headaches.

Stronger

Financial entities will be stronger or in other words more robust. Simply addressing reasonably identifiable circumstances will materially move the needle for a firm's cybersecurity posture.

In addition, there are at least three other provisions, which, if implemented without delay would strengthen firms' IT estate management, they are: (i) the right tools for the job, (ii) managing the ICT supply chain and (iii) managing the exit strategies.

(i) The right tools

Under DORA, financial entities shall use and maintain updated systems, protocols and tools that are appropriate to the nature, variety, complexity and magnitude of operations.

The move to Cloud is inevitable for a variety of reasons, but primarily the cost of installing and maintaining on premise solutions makes no commercial sense when compared with cloud-based solutions. The Cloud facilitates enterprise-class technology which is affordable and can be maintained, upgraded, and scaled up seamlessly.

Our increasing reliance on cloud has changed the playing field and it is critical that our businesses change with it.

DORA obliges firms to use tools that are reliable, and those tools must have:

sufficient capacity to process the data necessary for the performance of activities and the provision of services in time to deal with peak orders, message or transaction volumes, as needed.

For any business that is reluctant to move to the cloud, their hand will be forced by this provision.

(ii) managing the ICT supply chain

Financial entities may only contract with ICT third-party suppliers that comply with 'high, appropriate and the latest information security standards.' In other words, ICT third party service providers will be required to address reasonably identifiable circumstances and conform to best practice and implement global industry standards, such as DMARC.

(iii) managing the exit strategies

Financial entities must put in place exit arrangements with their ICT third party suppliers. This necessary provision reflects deep and extensive research and an acute understanding of the challenges that financial entities face and solves a real and painful problem for financial entities. In this instance, financial entities are the consumer, and it is right that the consumer is protected.

Occasionally, some ICT third party suppliers have behaved like squatters, when the contract is due to expire. Rather than facilitate their old client by removing their kit, making way for solutions that would serve the client better, either they claim that pulling out the old kit would disrupt business for weeks or they do disrupt the business. Needing to avoid business disruption the renegotiation of any contract is tilted in favour of the vendor (ICT 3rd party supplier) who has virtual carte blanche to increase their prices for kit that is no longer fit for purpose.

Bigger

It goes without saying that firms which can demonstrate that they have taken reasonable steps to address known significant cyber threats will be more attractive to investors and clients looking to protect their assets and data.

As a result, it is likely that those businesses will grow. It will provide those businesses with an immediate competitive advantage over the laggards who resist the changes.

Firms with a weak external cyber security posture will face compliance challenges. Furthermore, in all likelihood significant shareholders looking to protect their investment will insist the firm meets latest information security standards. Managers that resist can simply be replaced.

How will consumers and investors know?

For one, there is a new email standard that's about to drop any moment. It's called BIMI, it stands for Brand Indicators for Message Identification. BIMI will put consumers and investors on notice as to which firms have implemented DMARC and have taken reasonable steps to address BEC, the starting point for 96% of targeted cyber-attacks.

The combination of this piece of legislation and this new email standard will usher in a way for consumers and investors to make informed decisions about where they put their assets and commercially sensitive information.

Rois Ni Thuama

A Doctor of Law and subject matter expert in cyber governance and risk mitigation, Rois is Head of Cyber Security governance for Red Sift one of Europe's fastest-growing cybersecurity companies. Working with key clients across a wide market spectrum including legal, finance, banking, and oil & gas Rois writes and presents on significant cyber threats, trends, addressing and managing risks.