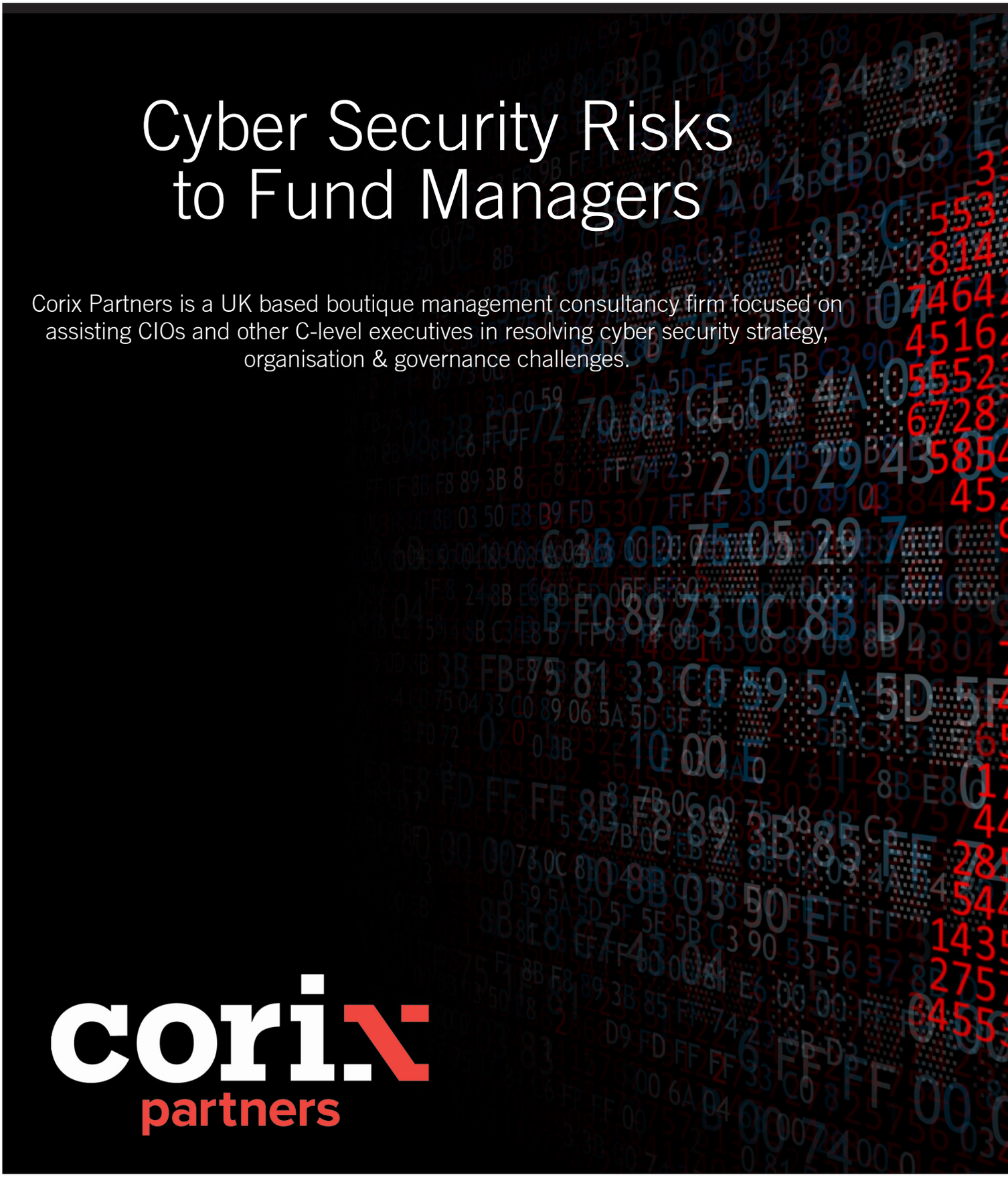
Cyber Security Risks to Fund Managers

Corix Partners is a UK based boutique management consultancy firm focused on assisting CIOs and other C-level executives in resolving cyber security strategy, organisation & governance challenges.



As Transformation experts with over 20 years of experience in the field, we help our clients develop strong company-wide Information security practices that deliver real and lasting value.

We believe that many organisations struggle with maturity problems around cyber security and that creating an effective practice stems from driving cultural and governance changes across the firm and requires long-term actions across numerous levels within the enterprise and relentless drive to succeed.

Corix Partners was established 2011 and we have since worked with a number of clients across industry sectors, mainly in finance but also in the logistics and leisure sectors. We are execution and transformation experts by trade and we pride ourselves in listening to our clients and helping them succeed at protecting their business better.

Cyber security threats are getting more and more sophisticated and the frequency of cyber-attacks has increased tremendously over the past decade. But the factor that has changed most recently is the amount of media, political and regulatory scrutiny on the matter.

A poorly handled relatively minor data breach can now have a massive reputational impact and result in significant loss of business. The UK Talk-Talk incident in October 2015 is to some extent a good example of that.

It is also key to realise that the traditional “bricks and mortar” perimeter of the enterprise has been long gone. Over the past decade, massive chunks of the IT estate have moved to the cloud and many aspects of business processes have been outsourced. A data breach affecting one of those service providers could also affect your clients and regulators are likely to take the view that it remains your responsibility as fund managers to ensure that your clients’ data is well protected wherever it may be.

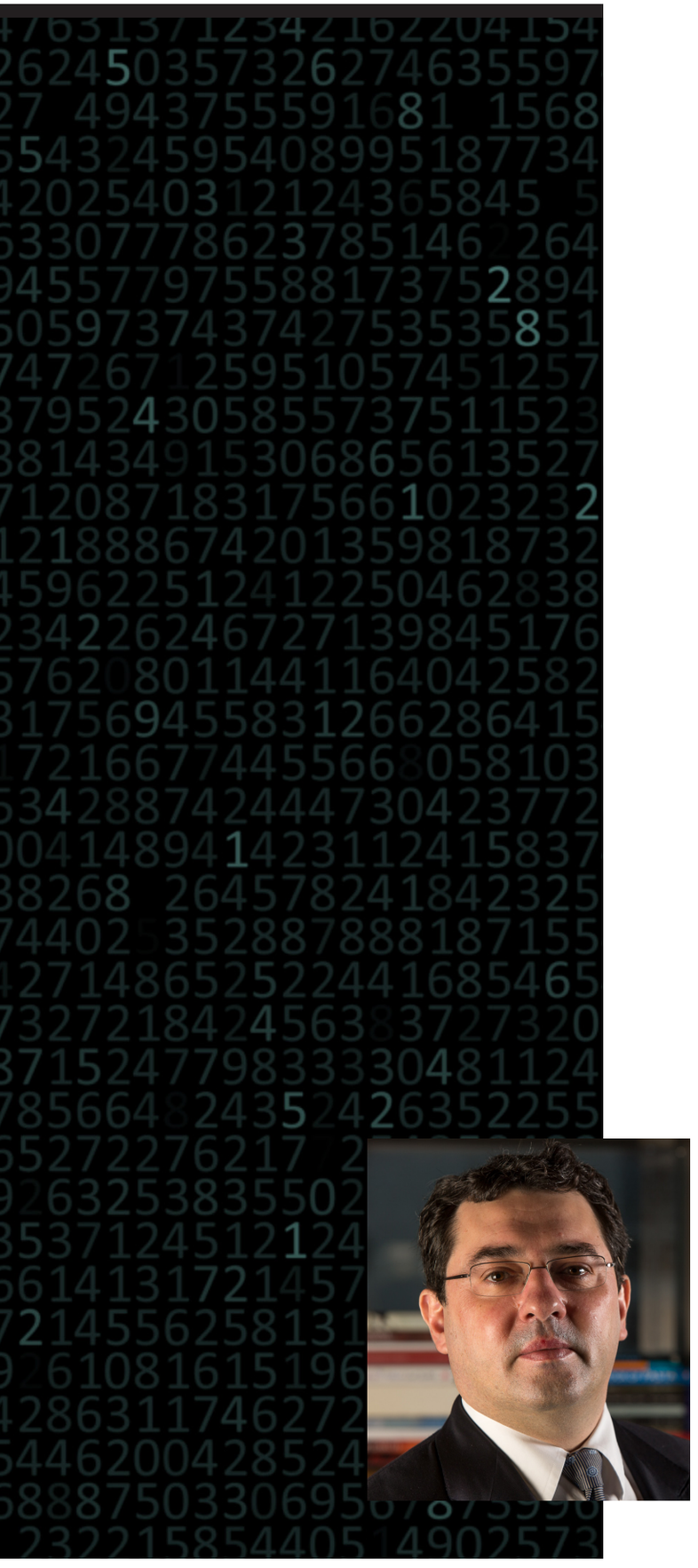
Cyber threats have a global reach and target all industry sectors. But the wealth management industry makes a particularly attractive target because it handles large amounts of capital associated with high profile wealthy clients, and is also home of a large number of relatively-small firms that maybe have not had information security at the top of their agenda for quite some time, and as a result many might have fallen behind in terms of maturity.

In regards to what kind of advice we can give fund managers and investors on cyber security in a digital world, multi factor authentication on specific transactions is a key good practice to limit the risk around online transactions.

Today, most people carry a number of digital devices with them all the time, and those can be used for extra authentication to make the customer experience feel more natural. For example, some credit card issuers use a one-time code sent by SMS text message to a registered mobile phone number to validate transactions that are deemed unusual.

This is a direction the wealth management industry could look into. The perception of customers is changing around those types of measures and it should not be assumed that they just wouldn’t tolerate them. This shift is driven by high profile data breaches and also by changes across society at large, which is becoming more and more digitally-savvy.

The key thing to bear in mind around cyber security is that cyber threats have not appeared overnight. In fact, they have been evolving for the best part of the last fifteen years and therefore there is a vast body of good practice that will go a long way to protect your business. But those good practices have to be in place, both within your environment and within the environment of your service providers.



Key examples of such good practices – in addition to the one mentioned before around multi factor authentication – involve the timely deployment of security patches, the regular security testing of key systems, limiting the usage of generic accounts or ensuring that production data is anonymised before being used in development environments.

Cutting corners around those on grounds of costs or convenience simply creates opportunities that cyber threats can target. This is increasingly becoming a matter of mindset, culture and governance. Sadly, we live in a world where prioritising convenience ahead of security can cost you more than you think. And cyber insurance should not be seen as a silver bullet, as insurers are likely to reject claims where basic controls are not demonstrably in place.

Supporting victims of cyber-attacks is an area we thrive in. We work with our clients to help them understand the real level of cyber security maturity at which they are at. When it is not driven by an incident or a near-miss, it is often driven by the arrival of a new senior executive at CIO level or above.

Cyber security problems are frequently rooted in decades of under investment or adverse prioritisation. It is key to work with all players within IT and elsewhere in the business and across the firm to understand exactly what needs to be done to protect the company at all levels.

We do not go into this with a fixed checklist or an IT agenda. We follow our own cyber security assessment framework and focus on listening to the specifics of each client and to their history with Information Security. We look at the specifics of their business and its true geographical and Internet footprint to assess the real cyber threats they face. We focus the assessment around the reality of each client to engineer acceptance of the assessment results and a true call for action.

Having established their real cyber security maturity posture, we generally help our clients build a transformation roadmap to address any shortcomings. For us, this is always about engineering lasting change, not just putting “ticks in boxes”.

Very often, this will go a long way beyond mere IT matters and will require a true cyber security operating model across the firm. It is also key to look at transformation with the right timeframes in mind. Changing mind-sets around cyber security takes time and it is almost always a mid to long-term journey.

Finally, once the transformation roadmap is articulated into work streams and projects, we have often been retained by clients to either take in charge some specific aspects of the work, or coordinate delivery across all activities of the cyber roadmap.

In our opinion, 2016 will see the continuation of the trends we have seen over the past few years around cyber security. Data breaches will continue to happen and attract wider media coverage. This will continue to push the topic up the list on board’s agenda. The key is for boards to stop treating the problem as a mere technical problem, stop looking for tactical silver bullets that simply don’t exist and face the reality in terms of necessary cultural and governance changes around security and across the firm.

Company: Corix Partners
Name: JC Gaillard
Email: jcgaillard@corixpartners.com
Web Address: www.corixpartners.com
Telephone: 07733 001 530