Leading Cyber Security from the Boardroom

Business leadership and security posture in the 21st century

A White Paper from:

Advent IM Ltd's Security Team

Introduction

Understanding cyber threat has never been more important for business leaders. High profile security and data breaches are regular news stories and the ramifications go way beyond the headline lifespan. Consumers are becoming more cyber security savvy and the perception of an organisation's security is featuring in where they choose to do business. A good example of this is TalkTalk, still struggling after two data breaches in twelve months, having lost many customers and now funding radical promotions to encourage users back. When we talk about the cost of a data breach, this ongoing fight back to reputation is not always considered, but it is an area that business leaders need a firm grasp of, if they are to successfully navigate the evolving and challenging threat landscape.

It is increasingly clear that a convoluted business ecosystem is a standard situation. This has changed organisational threat and risk in ways we have not seen before. Collaboration between cyber criminals is commonplace but in business this level of communication and collaboration is less common and is something we will discuss in this paper. The challenge is complex and evolving but with quality information and clear vision, the C-suite can contribute invaluable leadership and strategic thinking to cyber security at a time when it has never been more vital. Cyber resilience is a matter of collaboration not isolation.

Executive Summary

Communication between security teams and boardrooms is vital and the level of quality in communications clearly needs to rise, as does the level of security hygiene demonstrated by business leaders. Boardrooms will influence how staff behave and this needs to be considered a priority in terms of leadership.

The perception, both of the insight gained from cyber security reporting and what strategic steps need to be taken as a result, seems inconsistent and confused. Given the cost of failure in this area, the onus is on both security teams and business leaders to find a way to share information that can become actionable insight, as a matter of urgency. This requires a 'hands –on attitude' from the C-suite and, ideally, security representation at board level.

Many organisations are reporting an intention to increase spend in security in the coming year, but with the apparent disconnect with security personnel, where this increased budget will be spent and how its success will be measured is unclear. Risk needs to be reduced by activity and if there is no risk-based decision making around key business activities, processes, policies and platforms, then the organisation will not actively reduce its risk. The problem is not only that risk remains unaddressed but that security without a return looks like cost, and cost is the first thing to be reviewed for its reduction or removal.

Increased convolution of supply chains has increased risk for all members of those chains and ecosystems, and the potential to touch Critical National Infrastructure (CNI) is something that needs to be considered when security requirements of partners are stipulated. The business that is attacked may not be the target, simply a conduit to the target.

The impact of people on cyber security must never be underestimated and the threat they can represent can be turned into an organisation's most comprehensive front line of defence with good training and policy, which is not only enforced but demonstrated by senior management.

Culture

Peter Drucker, widely acknowledged as the father of modern management, once said, "Culture eats strategy for breakfast". When it comes to security, this could not be truer. An organisation may take great pains to build processes, issue policy etc. but if the culture is one that makes processes redundant and ignores policy, then that behaviour will eventually *become* the policy.

Consider how behaviour affects the way we perceive things in other areas of our lives. For instance, in 1983 the legislation requiring drivers and front seat passengers to wear seatbelts in cars, was passed. Now we would not consider driving without seatbelts because the enforcement of that behaviour eventually changed our culture and we now all happily strap ourselves in before each trip. The smoking ban is similar. For years, restaurants, cinemas and pubs were swathed in smoke and now, post 2007, it seems unimaginable that we would ever consider smoking inside these social venues. So the behaviour was enforced through legislation, the behaviour changed and then our behaviour became our culture. While we are talking legislation, the EU General Data Protection Regulation (GDPR) is due for adoption in 2018. Some of the changes this will usher in will have far ranging benefits for data controllers and organisations but there will be penalties to avoid. If this follows the same process as the areas we have discussed here, then the result will be an overall improvement of Data Protection culture, which is a key part of organisational information security.

Changing culture is hard, there is no doubt about that. The Personal Identification Number (PIN) entry door that has been propped open with a chair, the shared network login credentials given to a temporary worker or the PC with a password on a post-it note stuck to the screen; this behaviour starts somewhere and as the Chinese proverb says, "The fish rots from the head down". Boardrooms are being held increasingly accountable for the failures and misadventures that happen in their organisations and this is unlikely to diminish. Indeed, with changing legislation and the prevailing cyber threat landscape, this is set to grow. Poor culture very frequently comes from inadequate training. The trouble is that all too often, due to workload, senior management may fail to attend training when in fact, as the users of the most sensitive information and the guiding light of security culture, they need to be first in line to sign up.

Increasing spend on cyber security is on many board agendas and this is laudable. If the board has a firm idea of what it is setting out to achieve and what the return on that investment will be. It is also frequently a technical spend increase; software or a new platform. Training and awareness is frequently much lower in terms of allocated budget. (This is an important aspect of security and will be covered in the Insider Threat section). According to research, the UK has much less of an idea about what return on investment it is getting in terms of security spend, compared to the US, for instance.

Governance isn't easy, and boards are under increasing pressure and accountability across many business areas. Cyber security, however, is a universal growing concern and understanding the current landscape from the perspective of the board as well as supporting functions, such as IT security, is vital.

According to Thomson Reuters[1], boardrooms struggle to secure their own sensitive board information, and risky behaviour with potentially valuable information is quite commonplace. The problem was also apparent in the way the information was disposed of after its lifespan. (See Figures 1 - 3).

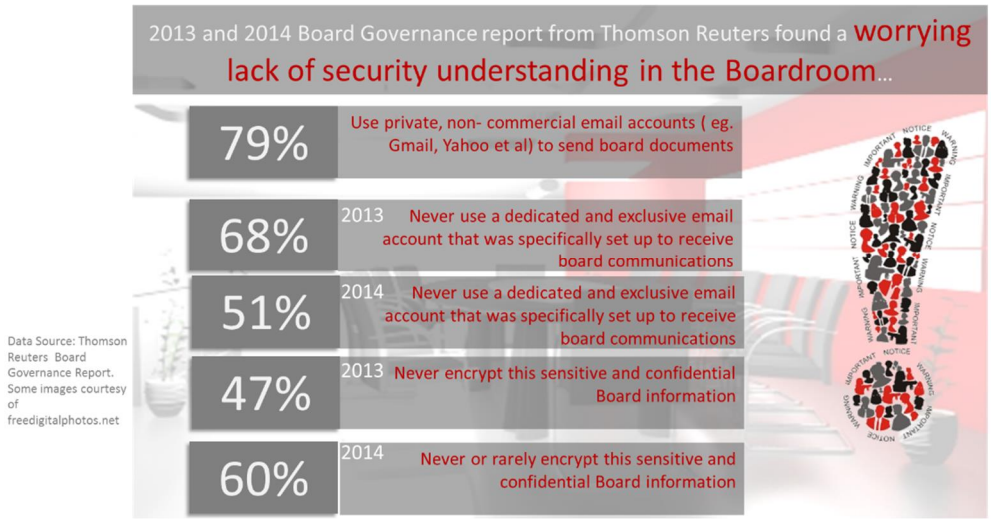


Figure 1

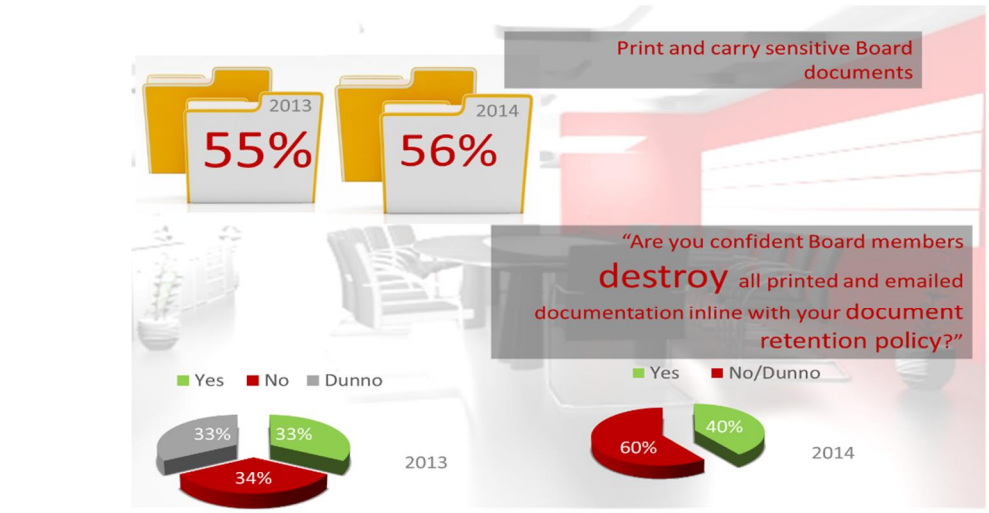


Figure 2

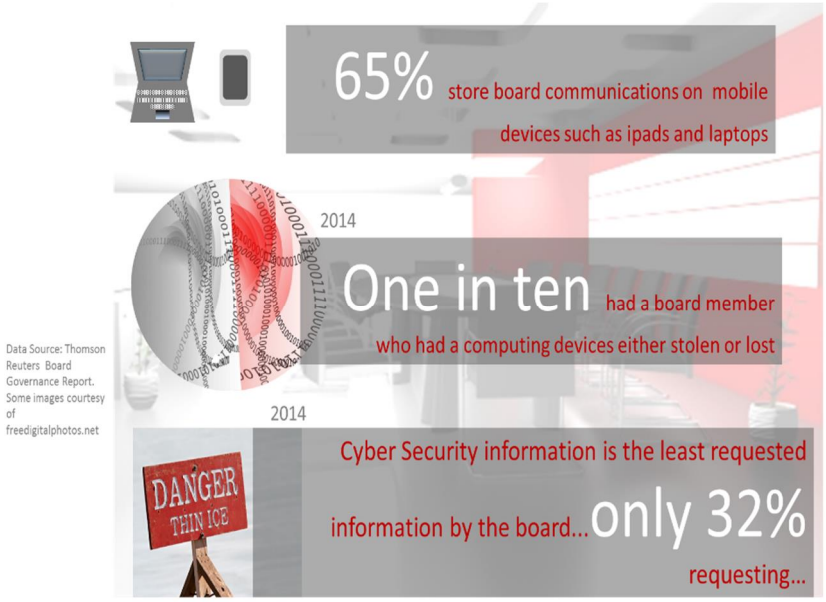


Figure 3

Data retention is a key area of Data Protection and, as we will see later in this paper, the regulation around this area is set to become even more scrutinised and tightened. Businesses that are already struggling in this area, with boardrooms displaying this kind of approach towards sensitive data, will find very challenging times ahead. Culture is a top down phenomenon and the attitudes and behaviours found at this level are frequently repeated and accepted throughout the organisation.

For such a key topic, it is worrying that such low levels of information are requested by boards[2]. But the topics of security breach and data loss are rarely out of the press, and the implications for the C-suite are becoming greater. The public and government alike are show increasing interest in the level of security in place at breached organisations and are holding Directors to account. TalkTalk, for instance, brought boardroom response to cyber-attack front and centre of UK cyber security awareness. The CEO, Dido Harding, found herself in front of the Culture, Media and Sport Committee[3], answering searching questions on exactly how the now legendary data loss occurred and why. Perhaps the interest was sharpened by the fact that this was the second data breach that TalkTalk had experienced in twelve months, causing serious doubt to be cast over their security posture.

Culture is set in the boardroom. The behaviours exhibited by business leaders will set the culture for the organisation. Make it a priority to ensure you get it right in the boardroom.

Security/Boardroom Disconnect

If we acknowledge that not all boards understand the importance of their own security behaviour, then we need to look at the reasons for this and look at the relationship between security and business leaders. Is it necessary for boards to have the same grasp of security as they do of other functions and units like HR or Finance? Well, the US has recently passed legislation that requires boards to reveal if they have a cyber expert as a member. Whilst it isn't explicitly saying you must have one, it certainly seems to suggest it is a good idea.

In reality, it would be difficult for every business to have an expert but a level of accountability and demonstrable capability in cyber security leadership, given the current landscape, certainly does seem like a very good idea.

Recent Bay Dynamics research[2] indicates that the perception from the C-suite of their understanding of the information they receive from their IT security teams, is very different from IT security teams' perception of how their information is understood or received. Whilst cyber security is not solely an IT function, this research gives us a good indication of the gulf between reality and perception in the boardroom. (See Figures 4 - 8).

Some organisations, however, are doing very well at boardroom leadership and are reaping the benefits that come with that, not only reputationally but in decreased levels of successful attacks. Firms that have an active C-suite in cyber security have experienced far lower growth in cyber-attacks across all major attack modes.[5] (See Figure 9).

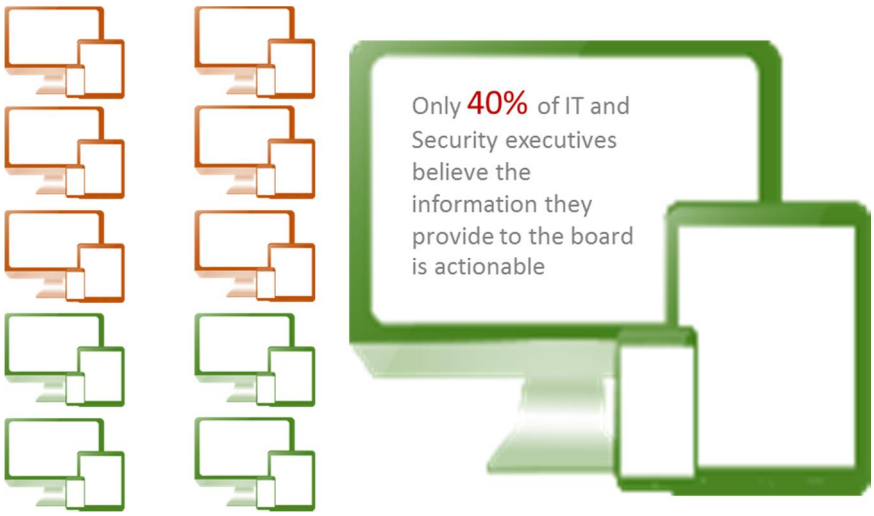


Figure 4

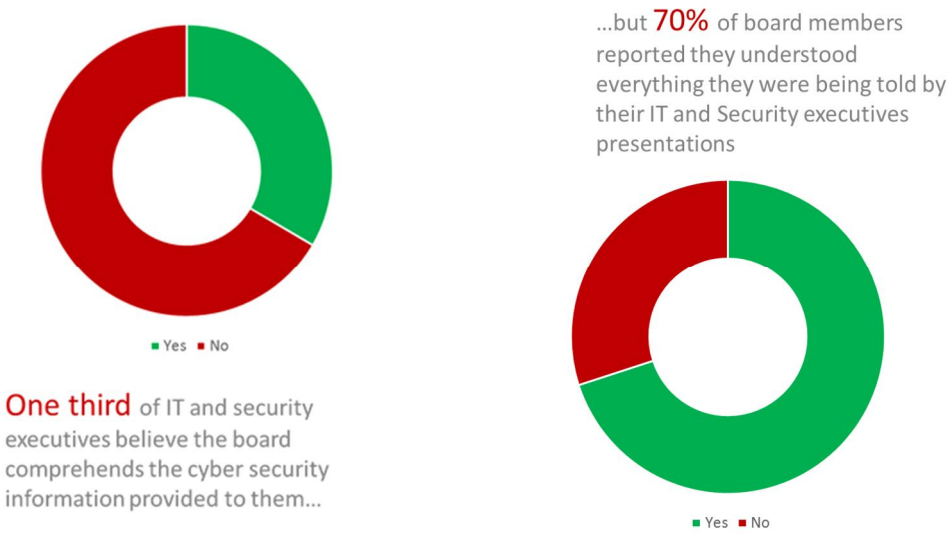


Figure 5

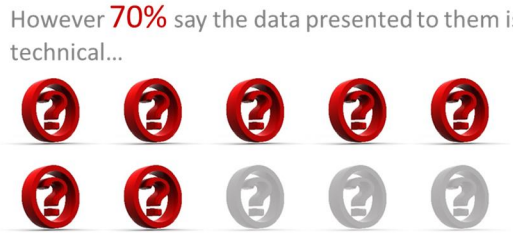


Figure 6

Figure 7

59% of board members say that one or more IT security executives will lose their job as a result of failing to provide useful, actionable information.

34% indicated they would provide warnings that improvements in reporting would need to be made.

Figure 8

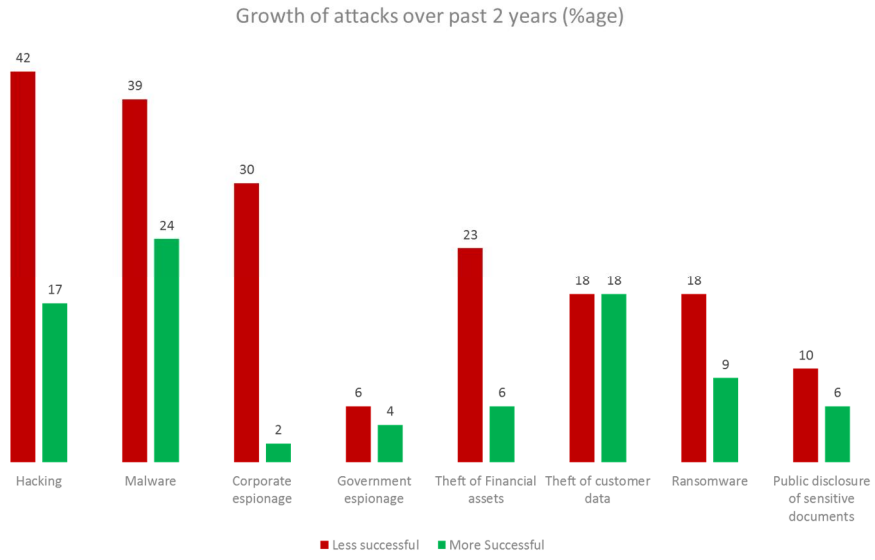


Figure 9

This research makes us question if boards really do understand what they are receiving and if they do understand, why some feel it isn't reducing risk. After all, there seems little point in continuing activity in security that doesn't reduce risk.

The last part of the research comes as an added worry when we factor in that we are in the midst of a generation-long cyber security skills gap[4] and firing security professionals rather than adjusting the way information is shared or disseminated, to ensure a strategy that does reduce risk, surely seems a better approach. According to The Economist Intelligence Unit[5], 58% of more successful firms (those with lower growth in cyber-attacks) are having difficulty recruiting qualified security personnel and almost half reported retention difficulty.

Security and boardrooms are not communicating effectively. The gap must be bridged before further risk is created and vulnerabilities created go on to be exploited and the inevitable breach occurs.

Business Ecosystem

Many businesses and organisations are acutely aware of their own supply chain. The cyber security of it may or may not be a factor in this awareness, but we know from the bitter experience of US retail company Target, that the supply chain can offer a serious cyber threat. One of the biggest security breaches in recent times came from Target, who were in fact attacked, not directly but through their air conditioning maintenance suppliers' portal. So, not only do organisations need to know their own business environment and what is connected or web-enabled to it, but also of their suppliers and the rest of the ecosystem in which their organisation exists.

Awareness of how third parties, suppliers, contractors and customers pose a threat to our own enterprise can only be established through a proper risk based approach, but research by Radware[6] reveals that not all organisations are taking the threat to the heart of their risk assessment culture.

Figure 10

The threats posed by our interconnected systems reach right through our supply chains and potentially into our CNI. Much of our CNI is in the private sector and, as the criticality of the infrastructure is relative and judged at the appropriate time against the Government's criticality scale, there is no common overarching approach or governance. This means that interaction or touch points with CNI in our own supply ecosystems needs to be of the highest standard. One could reasonably argue that this scrupulous approach should come as standard as part of organisational commitment to partner organisations, as at some point it is possible that any organisation could form part of a CNI supply chain.

Organisations need to understand the impact their security posture can have on partner organisations and the link to CNI.

Threat Landscape

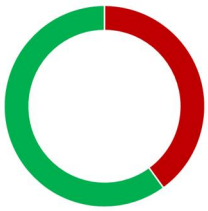
It isn't possible to cover *all* aspects of the threat landscape. However, the gap in organisational security focus on people, has been thrown into sharp relief by the rise of Ransomware.

Ransomware, according to Europol, is the dominant concern for EU law enforcement[7]. At the end of 2015, we predicted that this particular brand of malware would be the big security fail story for the next twelve months, and that prediction has sadly come true. Several families of malware are constantly doing battle in cyberspace of course, but ransomware families have proven to be lucrative and resilient for criminals, with everyone from individuals to NHS trusts and banks being threatened or attacked by criminals demanding a Bitcoin or other crypto-currency ransom to release illegally encrypted files back to their rightful owners. Though sometimes this part of the bargain remains unfulfilled – another reason to think carefully about whether you really want organisationally engage with cyber criminals. They may return to soft targets who pay up, again and again. Ransomware is most frequently delivered by phishing email or drive-by infection, and the reasons for this repeated and growing threat become apparent when we look at our employees.

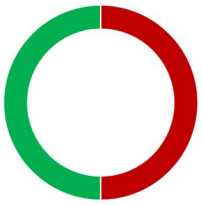
Insider Threat comes in many forms and for a long time our perimeter focus on security has allowed a large amount of risk from insiders, both hostile and benign, to flourish. We know that poorly trained staff represent a significant amount of threat to business, and staff, contractors or visitors doing risky things is frequently at the root of many security incidents that impact organisations. This could be behaviour such as opening and clicking phishing emails. As stated earlier, ransomware is frequently delivered in this way and if staff are not trained properly and regularly in how to spot and delete phishing emails, the threat from this malware will continue to grow. A security focus that does not take the human factor into consideration and relies solely on software to protect it from malware like this, will always be at a disadvantage as it will not benefit from the nuanced and on-the spot- reaction of a well-trained and alert staff member. A well trained staff member will not only potentially spot a phishing attempt and block the malware, but they also know that security policy when it comes to web surfing and will not visit websites that are designed to infect networks on a drive-by or watering hole basis. The second line of defence will be decent software, but it should never be the sole defence. Sadly, training is usually one of the poorest resourced areas of security, with a fraction of the amount invested in software solutions invested in people. This is a wasted opportunity.

Part of the associated threat from insiders can actually come from senior management or board members. As we established earlier, the boardroom does not always handle its sensitive information well and it is worth noting that these are very frequently quite privileged users. They may not be subject to some of the monitoring or policy that may impact other users, as their seniority may have placed them above this. However, in actual fact given that they are the users of such significantly sensitive or valuable information, they should be included in all training and policy as a matter of course. According to Vormetric[8], privileged users (which will include system administrators etc.) are the biggest threat group to organisational security, ahead of contractors and business partners. Executive Management are a serious threat to security too at 28%.

The UK has a highly developed concern about insider threat[8], according to Vormetric, and that has come from bitter experience of significant data breaches. It is reassuring to know that many have decided that the best route is to increase spend in this area. However, as we know much of the threat comes from people, we can only hope that this budget will include a significant increase in investment in training and education of employees, including board members and senior managers. All too frequently the busy schedules of these people has meant that they may quickly forego training, when in reality they should be leading from the front.



40% of UK businesses reported a significant data breach or failed a audit in the last year



50% are now looking to increase security and Data Protection spend in the next year

Figures 11-12

DDoS attacks, made famous by hacktivists are still a threat to business and recently a well-known security researcher had his website knocked down by an attack of unprecedented size. This attack was enabled by a zombie botnet made of Internet of Things devices that had been infected and co-opted to perform this attack. Securing devices and systems that sit outside of our corporate networks needs high level vision and leadership. They need to be included in change management protocols and given the appropriate level of protection as corporate networks enjoy. DDoS continues to act as a childish act of sabotage but also as a distraction for other, more sinister behaviour on networks.

Bringing security policy and protection to all affected areas of a business has to come from the boardroom as mandated policy and procedure to ensure it becomes culture.

Cyber Threat is not going to decrease. Indeed, the Internet of Things, our ever increasing level of interconnectedness, our work/life blend and many other factors are all conspiring to create further potential attack surfaces and criminals are very joined up in their approach to exploiting these factors. For business to survive and thrive in this climate our response needs to be robust and front-led. A confident and well informed c-suite is a vital component and an excellent starting point for cyber security success and enhanced reputation, commercial advantage and resilience

Sources:

1 Thomson Reuters Board Governance reports 2013 and 2014

2 Osterman research for Bay Dynamics

3 DCMS committee interview Dido Harding here http://www.parliamentlive.tv/Event/Index/73368590-d756-4a37-badb-8174ac8ef239

4 National Audit Office report February 2013 – It will take twenty years to fill the UK Cyber Security Skills gap

5 The Economist Business intelligence Unit – Data Security: How a proactive C-suite can reduce cyber-risk for the enterprise.

6 Radware – Security and the C-suite, Threats and Opportunities

7 Europol IOCTA report 2016

8 Vormetric Insider Threat report 2016

Figures:

1 -3	Thomson Reuters Board Governance
4-8	Bay Dynamics
9	The Economist Business Unit
10	Radware
11 – 12	Vormetric

advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM

bestpractice@advent-im.co.uk