In 2015, several high-profile security breaches kept the topic of cybersecurity in the headlines - and the next 12 months doesn’t look any different. As organisations look to change their business models to adapt to the digital economy, they’re also looking to change their security posture to defend against cybercriminals.

In an increasingly connected world - of social media, mobility, and cloud - the need for greater intelligence and insight will give businesses a stronger and smarter security stance. However, the complexity of the new digital environment is informing some radical new approaches when it comes to security in 2016.

‘...the need for greater intelligence and insight will give businesses a stronger and smarter security stance.’
Trend 1: Security steps up to meet the digital age

The chief information security officer (CISO) faces a new headache: digital complexity. The digital world has changed how organisations communicate with the world out there. According to Matthew Gyde, Dimension Data’s Group Executive - Security, the rapid increase in how we use technology to communicate has led to more data and more points of entry or breach, but because of the rapid pace, security hasn’t adapted fast enough.

“We saw this in the explosion of hacks in 2015,” he says. “CISOs will now have to have a hard look at new policies and processes to address this as an urgent item on the security agenda in 2016. Information security, like any other discipline, has to be re-evaluated and re-aligned as part of digital transformation.’

Gyde believes that social media plays a fundamental part in this journey. ‘People aren’t holding back on social media - they’re sharing more than ever before. Sadly, cybersecurity policies haven’t accounted for this. In the new year, these will have to gain alignment fairly rapidly as organisations strive for a greater depth of security. For example, a disturbing new trend is “whaling” - where hackers target senior executives with ransomware, demanding money or using their information fraudulently. The challenge is to protect an individual and not just their cyber presence.’

Forensics will be even more important in the coming year. As people use different types of technologies in the digital business, these technologies will all be increasingly subject to exploitation. As the stakes get higher, businesses will need to continuously scan the Dark Web as cybercriminals become more bold and deliberate.

‘The reality is that no business, no matter its size, can avoid security incidents anymore,’ cautions Gyde. ‘Instead, the business must be able to anticipate them, and have the capability to identify and respond to these threats, often in real-time. Many of our clients are seeing the value in outsourcing information security activities to third parties as part of their efforts to mitigate risk and bolster their defences.’

Trend 2: Cloud shatters the perimeter

As organisations move security controls from a traditional perimeter to cloud-based providers, the traditional corporate network is becoming irrelevant. The adoption of cloud platforms and security-as-a-service, will continue in 2016. Neil Campbell, Dimension Data’s Group General Manager for Security believes we’ll see CISOs moving more of their perimeter security controls to these platforms as part of the efforts to reduce their physical footprint and costs associated with traditional infrastructure.

‘When you’re able to turn security controls on and off as needed, and enable your security in real-time, there are obvious benefits but also hidden management complexities,’ he explains.

‘The perimeter was always considered the “catch-all” for critical applications and workloads - such as ERP, bespoke applications, intellectual property, and so forth. But the cloud has now shattered that paradigm. Users and their devices are no longer confined to a single location - and the same applies for the data they’re accessing. In fact, some applications may not reside in a facility or location that businesses even know about.’

The trend will be to start following, or tracking, workload applications and securing them wherever they ‘live’. In essence, organisations will need to replicate their on-premise security controls in the cloud. However, Campbell believes it’s important to keep in mind that these workloads and applications behave very differently than a network from a security point of view - they’re often a lot more unpredictable.

‘While perimeter security remains critical, security in the time of cloud and digital needs a new approach as we start to see an emergence of hybrid security infrastructures. The challenge, as we move into the new year, is to have policy and event management that can be controlled centrally, regardless of the location of the application or data.’

‘Many of our clients are seeing the value in outsourcing information security activities...’
Trend 3: Business adopts a ‘seize’ mentality

A year ago, we predicted a resurgence in interest in endpoint security. Security professionals were starting to take a closer look at their devices - whether a PC, Mac, smartphone, or tablet for indicators of compromise.

Because companies have allowed so many employees to bring their own devices into the corporate environment, traditional network-based security controls aren’t able to keep up. This is motivating many organisations to seize control of the security of devices at their endpoints without restricting a user’s mobility or productivity.

According to Campbell, the focus now will extend into applications and patching. ‘We expect businesses to start exploring methods to validate the safety of applications before allowing users to download these applications onto their devices. Identity will become more linked to the network as IT teams put individual users in the cross hairs: Where are they located? What information can they access? What device are they using?’

‘Some of our clients are already talking to us about leveraging a system where devices or endpoints can evaluate and “rank” local applications according to a perceived level of risk. We’re really moving away from a signature-based identity model to a proactive approach - where you can verify the “intentions” of an application before allowing it to be downloaded.

One thing we’ve noticed is that organisations struggle to create a business case for user awareness activities. We’ve worked with our partners to create a series of security awareness videos - called Inside Security - and we’re making these available to the community at no cost.’

For security professionals, the caution is: the critical applications and workloads you need to protect may not be on the network anymore. You won’t understand the masses of data traversing your environment in the digital era without intelligence.

‘We’ve worked with our partners to create a series of security awareness videos - called Inside Security - and we’re making these available to the community at no cost.’

Trend 4: Intelligence takes on a defensive stance - keep your eye on the target

Intelligence can’t be separated from any security initiative as we move into the next 12 months. With better intelligence, you can get smarter about security - taking a proactive rather than a reactive stance.

As Gyde explains, all too often, businesses fall victim to malicious attacks because those monitoring and control systems in place provide them with too little information, too late. ‘These traditional approaches of gathering intelligence tend to put you on the “back foot”, he warns.

‘Not only should your security allow you to anticipate attacks, but allow you to take the appropriate action. We believe organisations should take a “one-two punch” approach to intelligence. It’s important to keep your eye on the target and not on the ground. The first is to engage a managed security services provider - to give you information about possible or real threats to your systems. The second is to augment these insights with deeper threat analysis and reporting. And this is where data will give you a stronger stance.’

Most security professionals have masses of unstructured data at hand. The next step is to put this data in a structure that gives you a level of intelligence to make an informed decision on how to adapt your security posture. In this way, you’re making better decisions - and taking swifter action - based on the events you’re seeing in your environment.

Trend 5: Hypervirtualised, software-defined security - the appliance is dead, long live the (virtualised) appliance

If anything, 2016 is set to be the year of hypervirtualised security. ‘The firewall was always seen as the first and last line of defence for preventing threats, but this can lead to a false sense of security or, worse, an attitude of complacency,’ explains Gyde. ‘With workloads dispersed over the Internet, security professionals will need to think of new strategies to build - and secure - critical applications and workloads in a variable security environment. It’s about taking the physical hardware of the firewall, which is sold as an appliance, and making it a software-based entity. In this way, you start solving a software problem with software. As with software-defined networking, software-based security will help create an agile and flexible infrastructure.’

When you start to virtualise full-feature security workloads, you unlock true portability and cost efficiency. As vendors are required to deliver consumption models to their customers they may see their sales dip but then even out and become more consistent. While there may not be large once-off hardware sales, vendors will start to see more repeatable and predictable sales. Gyde believes that those businesses making their foray into the digital space will be reap almost immediate benefits. ‘Firstly, they’ll have more agility as there are no expensive assets to write off at the end of a cycle; secondly, they’ll be able to change their strategy to adapt to security concerns as they manifest in their own environments.’

Finally, he predicts that IT purchasing patterns of business will start to change in 2016: ‘In the year ahead, we’ll see businesses start to “take back” security into their own hands,’ he concludes.

- Top IT trends to watch in 2016: accelerating the digital business
- Top IT trends to watch in 2016: digital infrastructure
- Top IT trends to watch in 2016: hybrid cloud
- Top IT trends to watch in 2016: workspaces for tomorrow