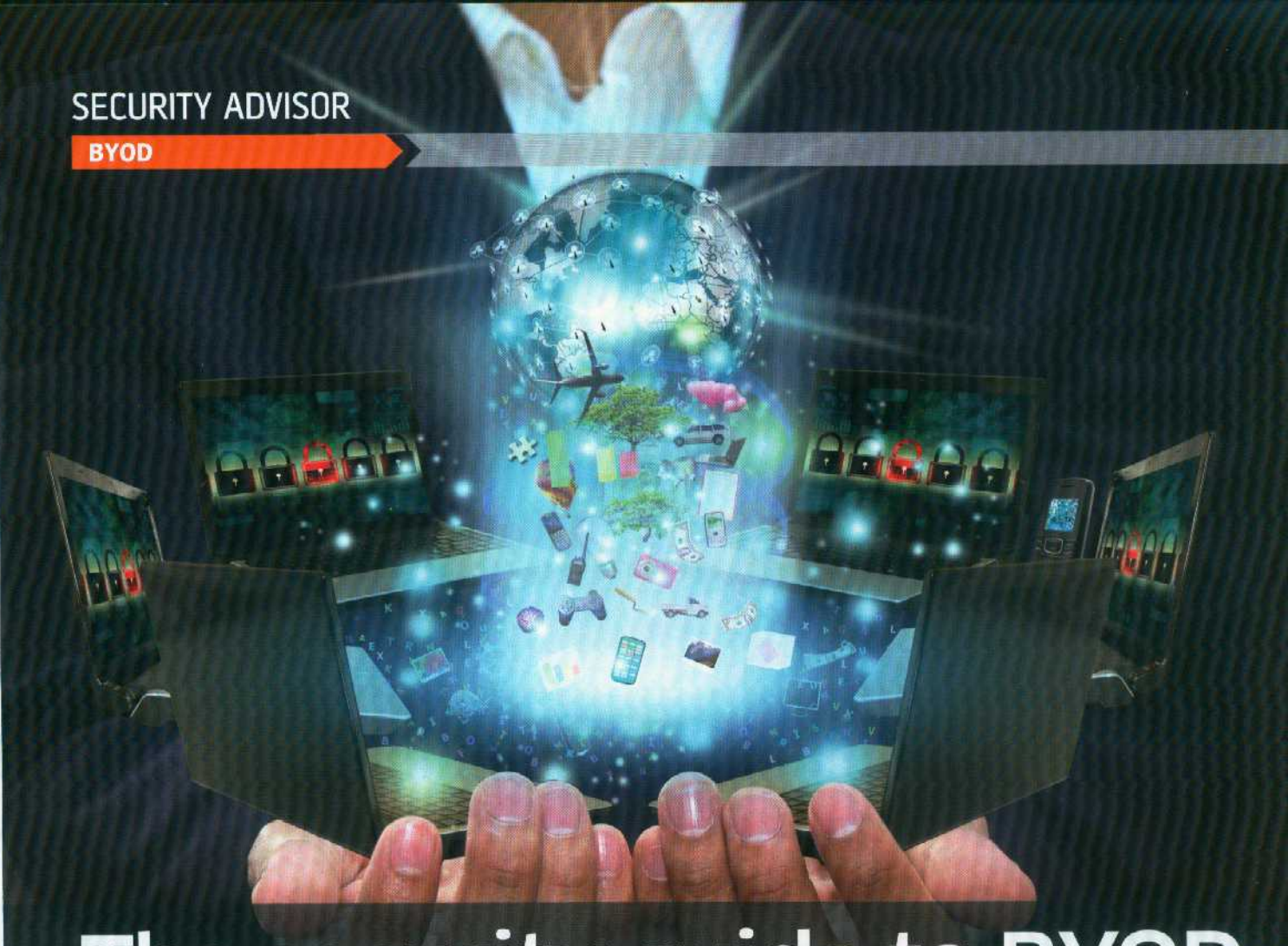

The security guide to BYOD

There's no use in trying to resist it – BYOD is here to stay. To help in the transition, *CNME* rounds up tips from the security industry on how to cope with the inevitable risks that the trend brings to the enterprise.

It used to be so simple. A new employee joined your organisation and you gave them a laptop, which was entirely under your control.

You could lock down the operating system to prevent the installation of potentially insecure or unapproved applications, and you could ensure the device was suitably up to date with your security solutions.

Weren't they the good old days?

Now, there are all these people telling you that employees should be able to bring their own devices to work. They say they should be able to access your beloved network with their shiny new smartphones and tablets that are apparently the best things since sliced bread.

As a result, your company has established a BYOD policy, enabling them to do just that - all in the name of mobility, which is supposedly something every CIO in the world should be embracing.

But these devices are corrupt. They're vulnerable and they're creating risks. The worst culprit of this is Android, which just so happens to be the most popular mobile operating system out there. This is a painful fact for any CIO when you consider that 99 percent of all mobile malware detections in 2012 were threats targeting Android devices.

"However, not a single platform is protected against threats such as phishing or loss of a device," says Konstantin Voronkov, Systems Management, Mobile Devices and Virtual Environments Group Manager, Kaspersky Lab.

"Loss or theft of an employee's gadget represents not a lesser threat to a company than malware infection. The loss of a device leads to a corporate data leak which may have negative impact on business. That is why IT staff must be able to control data remotely, for example, by blocking the lost device or by deleting all the information and mail stored on it."

So these mobile threats are real and costly, which Sowri S. Krishnan, Vice President of Mobility, Cognizant, more than testifies to.

"A lack of integrated mobile security is costing companies in terms of everything from lost productivity to lost data," he says.

As a result, transitioning to a BYOD model should be phased in over time. "Organisations need to mitigate security risks, such as inappropriate usage or loss of corporate data and the ensuing financial and legal implications," Krishnan says.

"Establishing effective governance mechanisms to ensure data privacy and security can be challenging when embracing a BYOD philosophy."

According to Florian Malecki, Head of Product Marketing, Dell SonicWall, different security practices apply depending upon whether the mobile devices are connecting from outside or inside the network perimeter.

"From a security perspective, tablets and smartphones are vehicles for information flow and so users may inadvertently - or sometimes even intentionally - relay malware into the secure network," Malecki says.

"Employees using their own devices could cause the network to be vulnerable. But nevertheless IT managers must at all times be able to guarantee bandwidth to critical applications while limiting undesired or dangerous traffic."

The good news is that implementing a BYOD policy doesn't require a complete redesign of an organisation's IT infrastructure.

"Many vendors and solutions providers have started to address these challenges and build a framework around them," says Hani Nofal, Director of Intelligent Network Solutions, GBM.

"By making sure that personal devices meet certain security standards such as Wi-Fi security, VPN access, and perhaps add-on software to protect against malware, a high level of security can be guaranteed."

Bulent Teksoz, Chief Security Strategist, Emerging Markets, Symantec, agrees, but says businesses should prioritise educating employees about mobile threats and protecting business-critical information that employees are accessing remotely.

"Businesses can use mobile device management (MDM) and mobile application management (MAM) tools to help maintain an inventory of the devices connecting to company resources and also make sure employees are adhering to policies. Reputable MDM tools also allow businesses to ensure both personal and company-owned mobile devices are wiped of business information if an employee leaves the company or a device is lost or stolen," he adds.

While a complete network overhaul is not required, the big question does remain – how much of an investment does it require to implement a secure BYOD infrastructure?

This is of course not possible to answer without knowing the exact details of each individual company, and as such the solution can vary considerably from case to case.

"This entirely depends on the starting point," says Mikael Hansson, Head of Delivery Management, Middle East, Ericsson. "The current status of the IT infrastructure will determine whether any company is in for a large investment or a relatively small one.

"Large companies with high internal and external requirements on information security, evolving from customer requirements, like SOX, tend to have a relatively robust IT infrastructure, which then would result in relatively marginal IT investments to secure the infrastructure for BYOD. Other companies might face considerably larger investments."

The main investments will be in extending corporate infrastructure, as well as operation costs, adds Alexander Zarovsky, Head of International Business Development, InfoWatch.

"To create a secure BYOD network," he says, "the organisation needs to expand its staff for proper administration of these devices within the network, which requires extra investments.

"There's also the up-skilling and -scaling of support personnel and network engineers, plus spend on applications to support things like performance monitoring and security tools. We estimate the extension volume to be around 20 to 30 percent for infrastructure."

Once that investment has been made and the implementation done, soon will come the time when management want to see ROI.

Such a thing for BYOD is difficult to measure because the costs and benefits are very distributed, and the potential cost savings found by not providing devices are often offset in management and support costs.

"Productivity benefits are often real but difficult to measure," Richard Marshall, Research Director, Gartner. "Extended day access to company email, for example, is very difficult to assess but can represent additional work per week for authorised staff.

"Providing direct access to work orders rather than field staff having to call in the office could save hours of travel time each week. The key is to define clear KPIs

99%

of all mobile malware detections in 2012 were threats targeting Android devices.


Haroon Iqbal, Sales Manager, MEA, Watchguard

and track them. Companies should not expect instant results as people adapt to new processes slowly."

Intel refers to its own example in early 2010, when around 3,000 of its employees were using personally owned smartphones. By the end of 2011, this number had increased to 17,000.

"We found that employees who were using their own devices gained an average of 57 minutes of productivity per day – an annual total productivity gain of 1.6 million hours for Intel," says Nassir Nauthoa, General Manager, GCC, Intel.

"The reason we witnessed such an increase in productivity is because users are usually more comfortable when working with a familiar device. They spend less time worrying about how to do certain tasks and are able to just execute them, which means a more efficient employee and in turn less time wasted for the business."

However, while more and more organisations in the Middle East embrace BYOD initiatives, Stephan Berner, Managing Director, help AG Middle East, believes most are still not tackling some of the biggest issues.

"The solutions I have seen are mostly around making sure there is a pin on the phone and that a user's phone can be remotely wiped," he says. "These are just sub functions of what a proper BYOD policy should consist off.

"Really, BYOD is about taking a holistic view of what happens to corporate data when it is traversing a non-corporate device and then understanding the threats that are imposed on it."

Despite this, the adoption and implementing of BYOD policies continues to expand, largely supported by the use of user credentials and access policies, independent of devices. Strong authentication and content security facilitate the adoption of logically defined perimeters, which include the realm of BYOD, according to Miguel Braojos, Vice President of Sales, Southern Europe, Middle East and Africa, SafeNet.

17,000

of Intel's employees were using personally owned smartphones by the end of 2011.

"We can say that BYOD is just a symptom of the changing landscape of corporate IT and its role in the company, from just an internal service provider to a business facilitator and stakeholder of the company success," he says.

It shouldn't be forgotten, of course, that the option still remains for CIOs to not let all employees bring their own device. Does the cost saving of not implementing a BYOD solution and security comfort outweigh the benefits of embracing BYOD?

"This is really a question every CIO needs to ask based on their business," says Haroon Iqbal, Sales Manager, Middle East and Africa, Watchguard.

"If a business has a large mobile workforce that needs to reach certain internal assets regularly, then adopting BYOD may have a high value - higher than the cost of adding new security controls," he says. "However, if a business has a large manufacturing team, where most of the employees work in a factory doing very specific tasks, perhaps BYOD offers very limited value, and is not worth the trouble."

Nader Henein, Regional Director, Security Division, BlackBerry, adds that companies which require their employees to travel a substantial amount of time are likely to benefit most from implementing BYOD.

"Companies which are encouraging the innovative use of technology in enabling collaborating amongst all of their teams will also benefit from giving their employees the flexibility in the choice of device they use in these innovative processes.

"The driver here, then, is executive and employee satisfaction, with IT then having to go and find a way of securing these solutions, which, more often than not, involves limiting their capabilities and tends to throw satisfaction back into a vicious circle."

Looking forward to the next year, organisations need to focus on monitoring and enforcing access to information and linking everything back to identity, says Geoff Web, Director of Solution Marketing at NetIQ.

"Employees within organisations, having had overly-restrictive MDM forced down their throats, have tended to revolt. Too often, these can also get in the way of business. It is more important to have a mobility strategy and manage mobile employees, not mobile devices." ■