Cyber security: How vendors are responding to the threat

By Lorenzo Zanni, Research Analyst IABM | 19 July 2017

If the threat of a cyber-attack is not yet keeping you awake at night, it is already a major concern for many broadcasters and media companies.

And if vendors haven't yet been asked about their product or service's resilience to cyber-attacks, they will soon.

The ever-increasing connection between back-office and front office systems makes not only media organisations' business systems vulnerable, but also their media assets.

You may not hear about such attacks often because the reputational damage is at the very least highly embarrassing for companies, but they are happening, with increasing frequency.

The attack on Sony Pictures Entertainment in 2014 may have been politically motivated, but such attacks can equally be for financial gain – ransoming assets for example, or obtaining customer personal and financial data for criminal exploitation.

Even a grudge or grievance can be the starting point for a highly damaging cyber-attack.

TV5Monde was the subject of just such an attack in 2014 – and was only saved from irreparable damage by good fortune – an engineer with the skills and knowledge happened to be on-site, and was able to identify and shut down the portal through which the attack was being conducted just in time.

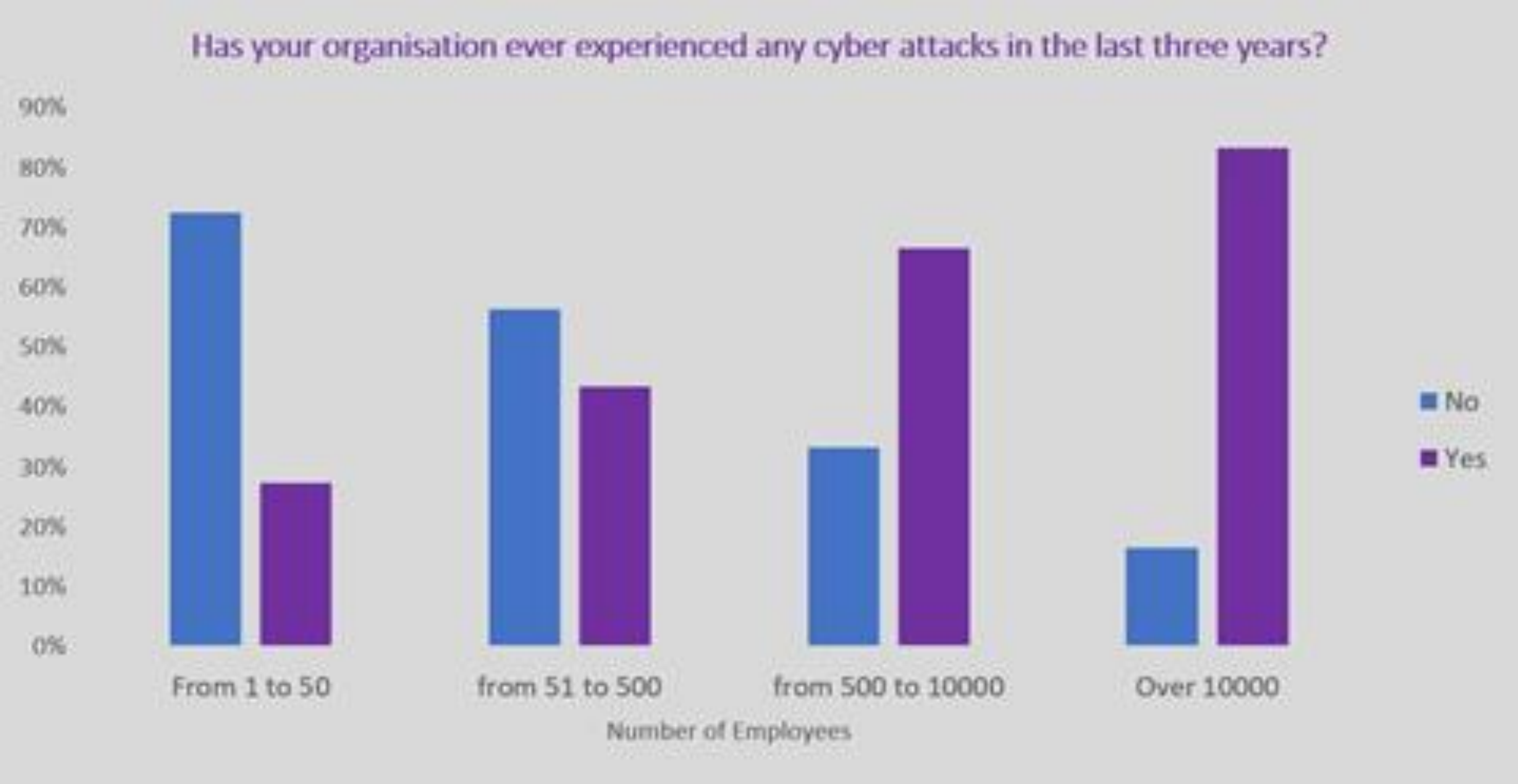
Broadcast under attack - protecting content and defending infrastructure - Thursday 20 July 4pm BST

Alongside theft of data and media assets, Denial of Service (DoS) or worse, DDoS (Distributed Denial of Service) is also on the increase, as organisations that don't share a particular broadcaster or media company's view of the world come under highly sophisticated cyber-attack in an effort to shut down their operations and damage their infrastructures and reputations.

Recently, there has been a growing number of well-publicised ransomware attacks where cyber criminals encrypt a company's data and will only release the key to unlock it following payment of a ransom – nearly always in near-untraceable bitcoin.

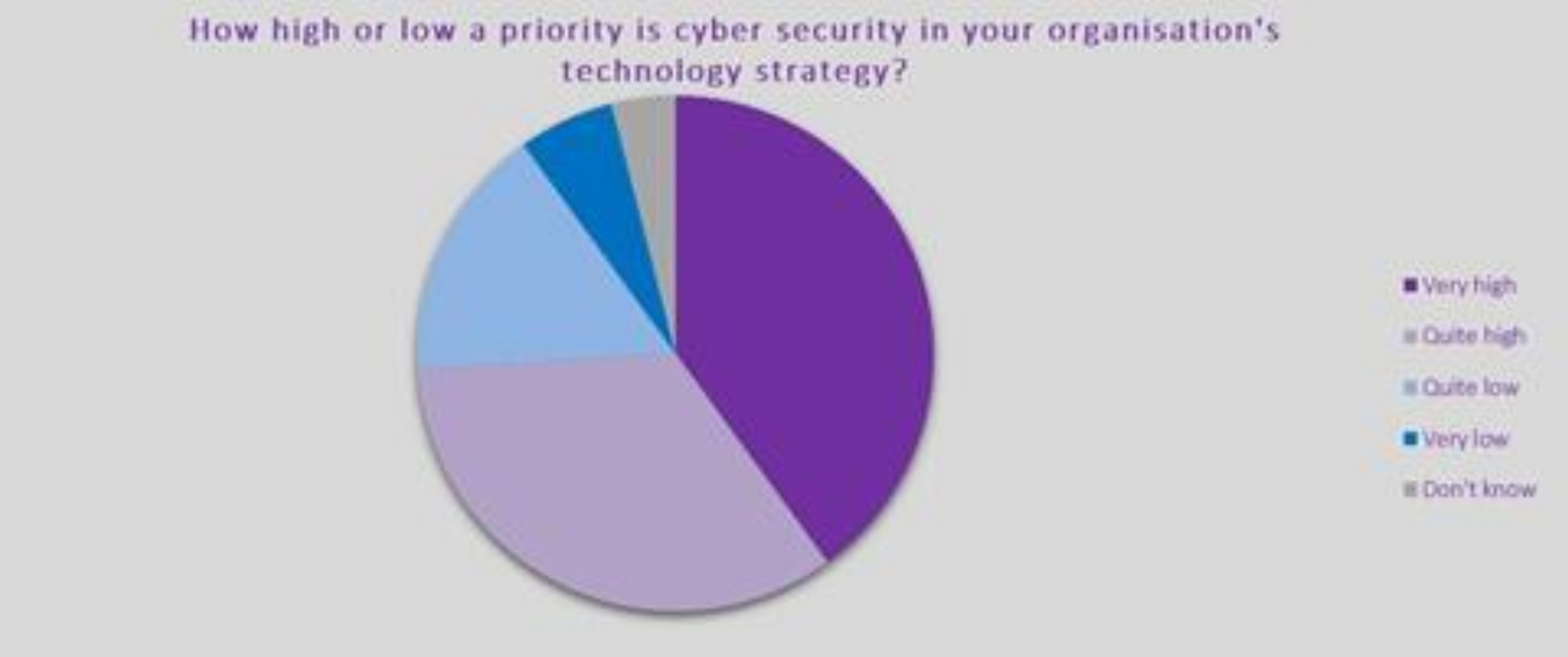
Out of date operating systems or security are often blamed for giving cyber criminals easy access; Indeed, in response to the WannaCry ransomware attack in May this year, Microsoft quickly released a patch for its antiquated Windows XP operating system to help protect the many people and organisations around the world who were still using it.

According to IABM End-User Survey data, company size matters a great deal in cyber security. In fact, most organisations with fewer than 500 employees have not experienced any cyber-attacks in the last three years while organisations with more than 500 have; for organisations with more than 10,000 employees the "yes" percentage skyrockets to 83%!



IABM Figure 1

Moreover, most end-users (74%) consider it a top strategic priority in broadcast and media technology procurement, as shown by the chart below.



IABM figure 2

Recognising this growing threat to its members' businesses, the EBU published a series of recommendations on cyber-security in 2016, including R143 – 'Cyber-security recommendations for media vendors' systems, software & services'.

Vendors already of course have to conform to environmental standards, while end-user broadcasting and media companies will soon start setting their own security standards, and the EBU R143 gives a good idea of what these are likely to contain. Most intrusions come through the back office, so a new level of cooperation is required between IT-based end-users and online technology suppliers.

"There can be no return to the bomb-proof days of SDI where there was no pathway between the VTR and the network" - John Ive

The cyber-security options for end-users range from using in-house resources to relying on their cloud provider.

It is perhaps counter-intuitive to use an outside resource, but cloud providers spend more than most individual organisations can afford on security – with hundreds of staff in some cases dedicated full-time to ensuring the security of their clients' operations; their business after all depends 100% on preventing problems.

Veset is one of the new generation of pure cloud playout solutions providers. "We see the industry trusting dominant technology players like Amazon (or Microsoft, or Google) to provide robust security infrastructure, which is built into their cloud platform," says Chief Executive Igor Krol.

"Our software sits on top of it and maximises the use of those resources. For individual broadcast organisations, it is tough to attract top talent IT professionals and maintain high-quality security systems.

"No system can give you protection from everything unless of course you switch off the internet and go back in time. However, there is no magic; either you build your expertise, and it has to be top notch and expensive, or you use the best in class providers, and they are in our opinion AWS and their peers," Krol adds.

Imagine Communications Chief Technology Officer Steve Reynolds agrees. "The cloud is more inherently secure than private data centers. Thousands of people at Google, AWS, Microsoft etc. have business cards with 'security' in their job titles – these companies understand how central security is to their and their customers' businesses. A broadcaster may have a full-time staff but not at the same scale."

SAM's EVP & General Manager, Media Software Solutions, Neil Maycock, also acknowledges that cyber-security is a growing concern. "For most of our systems the broadcast environment is heavily firewalled from the internet and the customer's internal IT systems.

"We are rarely engaged in the direct provision of security; our systems exist on top of the corporate platforms and policies. Our involvement normally involves ratifying the performance of our products on top of the client's infrastructure.

"However, we have recently had examples of customers asking us to complete questionnaires about our internal company IT security as part of their due diligence on suppliers. We expect this to be a growing trend."

IBC2017 Cyber security will be on the agenda at IBC2017, including Safety in Numbers: Collaborating Against Cyber-Attacks and Paper Session: Cyber and Content Security - Putting it into Practice

Imagine Communications has also experienced a marked increase in customer awareness on cyber-security. “This spans our full range of customers across origination, content creation, production and distribution,” says Steve Reynolds.

“All are worried about security because their platforms are now more open and better connected – which are huge operational advantages, but also bring security-related concerns.

“To address this, we look at security in three different vectors – content, network and process. If someone breaches network security we need to look after the content itself – with encrypted access control – AAA – authentication, authorisation and accounting. Securing the operations – i.e. the processing – is the next level.

”Can the intruder do anything to the bit streams? Every broadcaster has an understandable fear of an external agent being able to take their own content live to air in the broadcaster’s name.

“If you secure operations and have trust elements built into the system that control and manage and take corrective measures, then you can stop an intruder doing anything with the content.

“At Imagine, we’ve built a chain of trust – we know everything about every component – where it came from, how it has been changed etc. and we monitor this on a multi-level, second-by-second basis. It’s about having multiple points of control. You can never guarantee that something bad won’t happen of course, but it does mean that hackers cannot go to air on your back,” Reynolds concludes.

What can vendors do to reassure their customers that they understand their concerns over cyber-security and are adopting best-practice in this area?

“It’s only a matter of time before our customers demand security assurances,” says John Ive, IABM Director of Technology and Strategic Insight.

“Don’t wait for someone else to set the rules for security compliance – work on security now to get ahead of the curve,” Ive continues. “If you don’t embrace this early on, playing catch-up will be painful.

“There can be no return to the bomb-proof days of SDI where there was no pathway between the VTR and the network.

“To run a facility efficiently today, you need to know where everything is and what goes with it (metadata etc.) – so the back office simply has to be connected to front office operations; metadata must be visible to the back office.

“Our industry has become more like a media factory – measuring and recording all processes via the back office – and this is the way in for cyber criminals. Don’t leave the door open for them.”

Read more IABM’s articles on cyber security