An unprecedented wave of massive data breaches over the last few years has raised questions about the security and privacy of information held on any computer anywhere on a network, including that which is kept under lock and key at high-security data centres. One of the most recent high-profile examples is the attack on Sony Pictures, which was hacked in the run-up to last Christmas. Sensitive corporate data, as well as yet-to-be-released films, were suddenly made public. The incident led to the now infamous controversy over The Interview, the satirical film about a plot to assassinate North Korean leader Kim Jong-un. The US accused North Korea of the hack. It denied the allegations and challenged President Obama to show evidence of its involvement. This was largely ignored by The White House and instead, January saw the launch of a new initiative from Obama. Among other measures, he wants Congress to pass legislation requiring firms to inform customers within 30 days if their data has been hacked.

But even with the most stringent legislation, and with the rise of cloud and increasing amounts of enterprise data being held in data centres, how safe can information be from hackers?

“Cyber criminals are bypassing traditional perimeter security, even though companies have spent billions of dollars on it,” says Tim Eades, CEO of data centre security specialist Varmour. “Cloud computing and virtualisation are transforming the data centre and also creating more blind spots. You can’t protect what you can’t see.”

Robert Renzulli, director of global security operations centres at CenturyLink, agrees: “Data centres are still evolving and attempting to keep pace with emerging threats, just as they always have. That will never change and is perpetual in the internet age, regardless of cloud computing.”

The evolving nature of the threat

With cyber criminals launching ever more sophisticated attacks, it’s perhaps understandable if enterprises are more wary of trusting their information to data centres. Tony Marques, cyber security consultant at Encode Group, says it’s vital that, as a starter, cloud providers demonstrate compliance to baseline best practice standards such as ISO27000 and PCI DSS.

However, even with those certifications, the need to have the data close to the end user access point often outweighs security concerns. Brian Chappell, EMEA and APAC director of technical services for security firm BeyondTrust, says: “Cyber criminals are becoming more sophisticated in many ways. But it’s still concerning that the methods of initial breach still revolve around mechanisms that are largely preventable. Exploiting known vulnerabilities and phishing still represent a significant proportion of the successful attacks.”

While worries about security are often blamed for holding back the cloud market, this may not necessarily be a bad thing, according to Ark Data Centres. “Customers who were always serious about security have always been concerned,” says its CTO Jason Liggins. “But there are those who believe we may all be worrying a little bit too much. For instance, the Data Centre Alliance reckons customers are not wary about trusting data centres with their information, as executive director Simon Campbell-Whyte points out: “I would suggest it’s more likely that the opposite is the case. Well-managed and secure data centres are, in the vast majority of cases, far more secure than the general office environment. “But threats can come from many sources and many layers and links in the chain. Data centres are but one link, and organisations should check with their supplier if the data centre is appropriate for the data they are putting in it.”

Campbell-Whyte is more concerned about the physical security of a data centre.
A data centre’s primary security function is access control and physical security, making sure only authorised persons are granted access to the server equipment.

Specific attacks

A physical security breach need not be a daring, commando-style attack on a data centre. It could be a lot more mundane, as Mark Edge of SaaS provider Brainloop, explains: "Hackers and organised crime may hog the headlines when it comes to IT security, but enterprises need to make sure those headlines don’t distract them from a far more common threat to data security – their employees."

Edge says staff are often the unwitting cause of a significant number of incidents. “For example, the UK government’s 2014 Information Security Breaches Survey found that 58 per cent of large enterprises suffered staff-related security breaches and 31 per cent of the worst breaches during the year were caused by inadvertent human error.”

CenturyLink’s Renzulli agrees. He says the majority of publicised security breaches over the past couple of years mostly come down to security awareness and vigilance by the employees and professionals supporting the data centres. He adds that the natural response is to evolve and adapt to the additional threats posed by cloud computing.

When it comes to the specific types of attacks that have so far been seen, Renzulli goes on to say that they still traditionally fall into one of several categories: cyber crime that is usually for financial gain; data theft such as industrial espionage, electronic extortion, leverage, etc.; ‘hacktivism’; network-based attacks to cause disruption, destruction and denial of service; and those that are opportunistic. The latter typically involves the collection of sources for building or creating botnets, spannets, malware and toolkits that allow for access to devices and networks.

Possibly the worst kind of attack is the APT (advanced persistent threat), whereby an attacker gains access to a network and stays there undetected. “The average [APT] attacker is inside a company network for nearly eight months,” says vArmour’s Eades.

So the challenges faced by data centre network managers when trying to keep one step ahead of the cyber criminals are many and varied. Data and customer volumes are probably the “biggest headache” according to Steve Armstrong of IT security training organisation, the SANS Institute. "Data volume issues arise when new customers are provisioning systems and huge configuration changes – OS installs, database movement, or redeployment. Additionally, many customers move to cloud computing for the network bandwidth and therefore intend to move high volumes of data. Logging this data is a real problem."

He adds that sometimes what occurs in these types of jobs is NetFlow sampling, which can be problematic for security and incident response requirements. “Your chance of capturing a malware beacon in that is almost zero,” he warns.

BeyondTrust says cloud network managers have a huge responsibility. “They are bombarded constantly with huge volumes of data around breaches which could lead them to look for the latest technical solutions that promise secure environments,” says Chappell.

But he goes on to advise managers not to lose sight of the basic best practices that lay the foundation for a successful security strategy: “Good configuration management, effective vulnerability analysis and mitigation, least privilege user access policy, and comprehensive coverage for monitoring and reporting. Get the basics right, and identifying the next tool or policy requirements is a whole lot easier.”

“Deter, detect, deny, delay and defend”

But, as Liggins points out, there are "many more clever criminals than there are people protecting the data“. Which is why, perhaps, he likens the physical security of Ark Data Centres to a castle of old. "The walls are both high and thick, but breach them and there is another with different mechanisms of protection. Any breach of the first will be detected and responded to. And Ark data centres have many layers of physical security to deter, detect, deny, delay and defend the IT infrastructure of its customers."

While there are many solutions data centres can deploy to guard themselves against attack, most experts would agree that there is no simple answer. One thing the Encode Group recommends for cloud
service providers to have is a security operation centre capability utilising security incident and event management (SIEM). This also features auditing functionality to monitor the data centre’s internal and customer-facing compute and systems.

“Data centre security is woven into every aspect of data centre operations,” says Marques. “Data centre managers should therefore be familiar with perimeter, and inside the perimeter, defence strategy and deployment. They should have and maintain a good general awareness of the threat landscape – especially around APT.”

Renzulli says that while solutions and technologies vary they should always allow for mechanisms that provide protection at the mobile device, web access point, application and database layers. He advises an overall “in-depth defence strategy” that comprises people, processes and technology measures that can prevent security breaches, and provide an organisation time to detect and respond to a breach or attack.

According to Renzulli, a high-level network solution to guard against threat encompasses: round the clock monitoring; notifications and alerts; incident response; mitigation and remediation; forensics; and intelligence.

Chappell’s advice is to start with a comprehensive vulnerability management solution, and to eliminate as many of the well-known exploits as possible.

“Combine that with a rigorous configuration management approach so that every system is deployed in a secure state. And then monitor that configuration to ensure there’s no ‘drift’ over time. Establish a real least-privilege approach to access for not only your own staff but those of customers as well – that will limit the opportunity for hackers with newly discovered exploits. An efficient SIEM is a must,” says Eades.

The SANS Institute offers more specific guidance. Armstrong says client isolation (through strict, well-configured virtualisation), network isolation of vLANs, and NetFlow monitoring of all physical and virtual routers should give some protection and remediation options. “Monitoring of client-to-client connections is a good way of detecting internal attacks,” he adds. “However, configuring the IDs for that is exceptionally hard and a continuous project as clients arrive, leave and move.”

A view to a skill

The solutions may be available but do data centre managers have the skills needed to counter the hackers? Here, the prognosis seems to be that while there are many skilled people in the industry, the threats they face are too varied and complex to be easily thwarted.

“The skills necessary to counter hackers and criminals are multi-disciplinary and specialist,” says Liggins. “It is unusual to find all such expertise in one person. Network managers need to have knowledge of all the areas that a hacker may use, and employ a range of experts to implement and monitor the counter measures.”

Chappell believes that most data centre managers have the skills to identify threats, and employ the tools and teams necessary to secure data centre environments – it’s just a question of priority. “They may not always be given the time, funds or resources to do so, and that’s an issue not only with senior management but also the data centre managers themselves. It’s important that in any security project, all the stakeholders are committed to its delivery, and fully understand and agree with the need.”

Armstrong echoes some of this: “Many of the larger data centres do indeed have the skills. However, they are not common and many of the smaller organisations simply don’t have the time, staff or skills to match a determined attacker.

“This is often a balance of service too, as the smaller centres are more likely to give a more personal service to the small buyer. So while options and configurability are wins for the small provider, the lack of security skills is a negative feature. That said, the view of many small businesses seeking a cloud provider is that they believe [an attack] will not happen to them, and that they will ‘cross that bridge when it comes’.”

While it seems that data centre operators may be reasonably confident of their defensive capabilities, others have less confidence in an individual organisation to adequately protect its own information. “Unfortunately, companies lack the skills and resources to successfully prepare for and address cyber security,” says Eades. “Therefore, data centre managers should be seeking a solution that simplifies security management and provides a consistent layer of security across all of their assets.

“Security has to be less intensive to manage. Managers can’t manage thousands of policy rules on each machine. It has to be automated. Security should be provisioned with and follow the workload through its lifecycle without manual intervention.”

As complicated as the security situation is at the moment, Renzulli believes people will adapt to meet any challenges, just like they have always done throughout human history. But this won’t happen automatically.

“Data centre managers themselves should have security and protection awareness knowledge. They should make sure that their teams supporting the data centres are consistently trained, and collaborate with the appropriate security teams for the in-depth security skill set to counter hackers.”