Simarjit Chhabra
CIO, Xtralis

> Physical penetration offers the hacker or the malicious user access to sensitive data.

We delegate. We outsource. We don't think it will happen to us. And not taking ownership of the security issues that face us leave us vulnerable to vendors who are more than happy to sell us security products and services on the basis of fear rather than reality.

Before we do a reality check on our own business and take stock of the situation, let's talk about the primary issue that needs to be fixed across the industry.

The infrastructure and applications for most business reside in a data centre whether you own, lease or host them.

Most of us take pride in our data centre and are proud of the fact we designed them from the ground up. We all have stories to share about the challenges we faced in building one right -- from seeking approval to dealing with vendors -- and a few of us could tell horror stories about the issues that resulted in time, scope and project delays.

We may rarely admit but we do forget to realize and do at times knowingly or unknowingly compromise on security aspects which are the reason why most Data Centres exist.

I want us to reflect deeply on whether we have implemented some good data centre practises or whether we have left it to others to figure out how to protect our information, which is the lifeline to our business.

Before we act, it's important to understand the "Defence-In-Depth" security model in which physical threat vectors often create the most vulnerabilities and are overlooked. In this article, we will discuss some of the good practices to implement while designing a secure data centre.

Physical penetration offers the hacker or the malicious user (even with less technical acumen) access to sensitive data, making it a very tempting attack method. Social engineering, shoulder surfing, and physical access to console ports are all facilitated. Dumpster diving by definition involves a breach of physical security. People are not the only physical threat. It may come as a surprise to some that even disaster recovery falls under the purview of physical security.

In most cases, information security specialists and their management teams will need to ascertain their organizations' needs for

> It's imperative that security not be treated as an afterthought when designing data centres.

physical security versus the costs involved. A small enterprise will have to either lease space from a data center or place data center space in a building with other offices. However, not many keep the risks associated with data centre on the company risk registers.

It was earlier a job of a facility manager to design a data centre and hand it over to the CIO/IT head of the organization. However, things are changing and evolving continuously. The role of facility manager has diminished largely as he/she doesn't invest in making changes in the data centre as often as IT staff change their line of servers. Let's review this statement – most of us have servers under 3 to 5 years old, but in some facilities, including Aircon, UPS, and cables may be more than 20 years old.

It won't be a surprise when power management comes under the IT umbrella in the near future. Yes, I predict that the CIOs of the future will be dealing with power management as each company will be accountable for power usage, the majority of which is used by data centres. The IT industry has the same carbon footprint as the aviation industry. CEOs will be mandated to report their power/energy consumption to shareholders and the stock markets in terms of carbon units.

It's imperative that security not be treated as an afterthought when designing data centres. Trial and error is no longer an option, as a single vulnerability can compromise the lifeline of any organization especially today when we all depend on technology to gain superiority over our competition.

In such a high-stakes environment, only specialized expertise is acceptable. We all deal with daily challenges surrounding encryption, certification, directory, network, and other security components that enable what one would consider a 100 percent secure network.

While the entire industry struggles with developing the technology to provide these protective measures, let's review some of the good security practises related to our data centres that we can implement to reduce the imminent risk to our business:

Site Location

• In order to reduce the risks from natural disasters, which include but are not limited to forest fires, lightning storms, tornadoes, hurricanes, earthquakes and floods, the site should be located where the risk is acceptable

• In order to reduce the risks from man-made disasters, which include but are not limited to explosions, fires and riots, the site should be located where the possibility of a man-made disaster is low, e.g., the site should not be adjacent to airports, banks, refineries, pipelines, etc.

• Location within the building should not be easily accessible to visitors or to the general public.

• Away from external windows or walls — best if it is centrally located inside the building

• Away from water pipes or other support system facilities

Regulatory Compliance

• The site should conform to or exceed applicable local structural building codes utilizing standards such as bullet proof glass, fire doors and reinforced walls and complying with disaster proof design:

- *Comply with all local zoning ordinances*
- *Certify not located in a 100-year flood plain*
- *Earthquake and hurricane bracing on all racks and cable trays (where appropriate)*

• Combined fire protection and smoke detection that meets or exceeds that of local fire codes and AHJ's (Authorities Having Jurisdiction).

– *"Very Early Warning" Smoke Detection Systems*

– *Gaseous Fire Suppression systems*

– *Very Early Smoke Detection/Gaseous suppression zones under raised floors*

• Limited number of building entrances in compliance with local fire ordinance

Physical Requirements:

• Preference should be to construct the room as a single unit.

• Walls should not form part of an external wall of the building.

• Roof, floors and walls should not form part of a common barrier to an adjoining area where the security administrator does not have security control.

• Walls should extend from the floor to the underside of the above floor slab (slab to slab). This ensures that intruders cannot enter locked offices simply by climbing over the walls and that fires cannot sweep unrestrained through the area

• If using glass as an external wall barrier, use shatter-resistant glass to limit damage from breakage. For some organizations, glass walls provide a sense of security because they can view who is in the server room at all times. For other organizations, the same reason may increase the security risk.

• Flood sensors and monitoring under raised floors and in other critical areas

• Separate grounding systems to prevent grounding loops; true ground versus green wire ground

• Formalized physical facility preventive maintenance program

• Ensure the dry pipe system is zoned and programmed to release water only under certain conditions.

Doors

• Doors should be solid core and not open out.

• Door hinges should be fixed to the frames with a minimum of three hinges per door.

• Door frame should be permanently fixed to the adjoining wall studs.

• Review emergency exit door locking mechanisms.

Power Supply

Mains

• Multiple physically separate connections to public power grid substations. Electricity must be received from two separate substations (or more), preferably attached to two separate power plants. There must be connectivity to more than one access provider at the site.

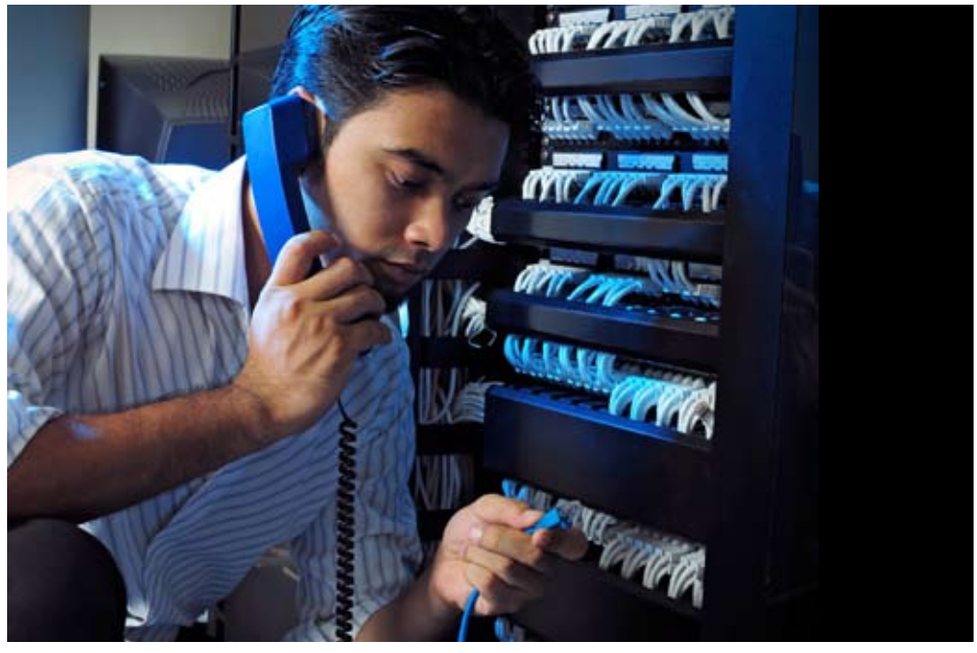
• Backup power supply needs to be tested on a regular basis.

• Electrical facilities that support the data centre should be separate from the main building.

• Electrical closets should be properly secured.

• Cables and wiring should be properly secured and tested to ensure adequate power supply.

"Threats can occur actively or passively from events either outside and inside the data centre itself."



> Threats can occur actively or passively from events either outside and inside the data centre itself.

UPS

• Continuous power supply with backup uninterruptible power supply (UPS) systems:

- *Adequate UPS capacity including air conditioning and lights*
- *UPS systems tested at full load on monthly schedule*
- *Fuel for UPS generators (48 hours worth) kept on premises and monitored for local environmental compliance*

• Power filtering in UPS system

Emergency

• Emergency lighting capabilities should be provided.

• Locate emergency power-off switches near all exits.

• Protect an emergency power-off switch from unauthorized use by encasing it in a clear plastic covering.

Heating, Ventilation and Air Conditioning (HVAC)

• Adequate multi-zone air conditioning, including a backup system for the multi-zone air conditioning

• Should be on a separate system from the rest of building

• The size of the ducts and vents should ensure that they cannot be breached by an intruder.

• There should be separate temperature and humidity controls in the computer/ server room.

• Positive pressure should be maintained.

• Ducts may require some type of barrier bars.

Physical Security

• Provide access to limited and managed security policies for all facility entrances

• 24x7 onsite security guards

• Visitor-logging procedure

• Card-key, biometric, or similar entry locks

– *ID-badge system for all employees and visitors*

– *Staff and visitors must wear badges at all times on premises*

– *Individual cabinet locks; master in NOC; key list from customer*

• All visitors must be admitted through reception with written statement of work upon sign-in.

• Written security policies readily accessible

Fire Detection/Prevention

• Install fire systems/ very early warning detection equipment.

• Install water/moisture sensors under the raised floor

• Have documented and tested emergency plans

• Deploy portable extinguishers at exits and near equipment.

Access Control

• Depending on the sensitivity of the information being processed, some type of electronic access control may need to be installed. This includes badge / smart cards or biometric devices.

• Alarm doors/area during non-working hours

• Have visitors sign in to document who was in the room and why they were there (i.e. maintenance, meetings, etc.)

• Have access control policies for daytime use, after-hour use, or during an emergency

• Enforce strict key control for locks. Door locks should provide both daytime locks, such as push-button locks (while the room is occupied), and 24-hour locks, such as deadbolt locks for after-business hours. Secondary access doors should be securely locked from the inside to prevent unauthorized access. Lock combinations should be changed as appropriate (i.e., every six months, whenever someone leaves the data centre, etc.).

• CCTV to view visitors and record their movements in all sensitive areas

Equipment locations:

• Video surveillance and motion sensors for entrances, interior doors, equipment cages, and critical equipment locations within the building

• Locked cages with ceilings; locking cabinets with climate control for those wanting more privacy

• Individual cabinet locks; master in NOC; key list from customer

• Secure rooms available

• Backup lighting systems for entry ways and cable vaults

Cabling

• All cabling designed to IEEE specifications (to support the required data rates)

• Communications cabling raceways separate from electrical; no intersections

• Shielded cabling as required for various application uses

• Sealed cable vault entrances to facility that are remotely monitored

• All cable runs physically protected from damage via tie-downs or where appropriate in conduit

• Fibre enters the data centre through diverse conduits or routes

• Multiple riser conduit from cable vault to data centre

Network Security

• Managed firewall services with 24x7 monitoring available

• Network security infrastructure in place:

– *Perimeter protection (firewalls, filtering router)*

– *Intrusion detection*

– *Authentication and authorization*

– *Backup and recovery systems to restore after a problem, such as load balancing, failover protection*

– *Regular assessment of network infrastructure*

– *Assessment of network expansions or additions*

– *Tape or media storage offsite backup*

– *Regularly scheduled security audits*

– *Server antivirus software protection*

• Written network access security policies readily accessible:

– *Password policies (such as not sharing, lengths, forced renewal, aging)*

– *Documented user responsibilities on security in company policies and reenforced by education*

– *Asset protection*

Operations

• Database of all installed equipment and configurations

• Toll-free telephone support

• Supported monitoring:

– *24x7 monitoring of dedicated servers and network equipment (note both frequency and method, such as PING, Simple Network Management Protocol*

– *24x7 monitoring of the health of the equipment with alarms and pager alerts for network failure and failovers*

– *24x7 monitoring firewall services available*

– *Alternate NOC available*

– *Second-tier support personnel located nearby*

• Trouble ticket processes:

– *Created and logged for all unusual or unexpected events*

– *Automated case escalation procedures in place, including escalation timeframes*

– *Reporting that provides trending statistics on trouble tickets and minutes (above) to facilitate quality and customer reports*

– *Performance reporting and end-user impact monitoring*

– *Periodic and exception reports provided to customers (including usage and problem reports)*

• Spare equipment on site for key networking equipment available in case of hardware failure

• Business continuity plan:

– *Daily site backups*

– *Tape vaults or other secure storage facilities on site in case of natural disaster*

– *Onsite and offsite storage available*

• Customer callout and escalation database with written procedures for each customer on alarm handling

• Each carrier has a secure termination area and location supported via the NOC or the carrier providing the termination

• Network security team in place

• Switching and links entirely redundant with no single points or paths of failure

• Intrusion detection implemented with automatic notification of intrusion attempts in place

• Switching and links entirely redundant with no single points or paths of failure

• Caching systems implemented

• All servers dual homed with load balancing implemented

Please note that some of the risks on the list may not be relevant to the particular data centre being tested. For example, a fence around the perimeter of the building is not practical in an urban setting. The checklist items listed as MUSTs are therefore few and far between and are only listed because, without them, very few other security measures would be of much use.

Information security specialists will put different weight on different items in the checklist according to their own organization's needs. This checklist is not a comprehensive physical security checklist. It merely provides a reasonable starting point in regard to physical security for a data centre.

Do remember to always obtain written permission from your management before performing security testing of any kind. Ensure that all the testing performed (physical penetration, fire control, social engineering) is outlined explicitly in the permission received from management.

Data centre management may require that a non-disclosure agreement be signed because of the potential exposure of security procedures. This checklist, as designed, only covers the physical aspects of your security setup. You will need other checklists to secure networks, operating systems, applications and other potential targets.

While designing a data centre, it's important to realize that they do not solely provide the "five 9s" of availability (99.999%). Security, scalability and manageability must be design objectives also because business today requires that each of them be considered from a complete, end-to-end perspective.

Clients or users connecting to the data centre measure performance by timely access to the desired application data, whether the connection is point to point or via an Internet connection. The user must perceive reasonable response and connection time. Access is no longer measured solely on an arbitrary measure of "network availability" or ping times.

While we have focussed our discussion on security, let's touch briefly on other three design criteria:

> "A complete network security solution includes authentication, authorization, data privacy, and perimeter security."

> It's important to realize that we need to be prepared for ever-changing environments.

Availability: This factor is generally ensured by the overall design of the network and can be implemented in several ways. Primarily, the infrastructure is designed to minimize the occurrence of service-related issues and the time to recover from incidents. Care should be taken to design high availability at each layer of the open systems interconnection (OSI) reference model with redundancy and failover provisions planned at each layer. The most effective solutions are those with consistent engineering considerations tightly integrated throughout the data centre, rather than those approached with a series of "piece meal" products and techniques.

Manageability: Many have a conception that management is about knowing if a server or other network element is "up or down." In the case of a data centre supporting multiple customers, it's defined as an ability to assess service level for each customer, which is essential toward administration of service-level agreements (SLAs).

It covers management of IP address assignments and tracking network configurations among other activities related to network operations centre (NOC) support systems.

It's important to invest in good manageability tools and qualified staff supporting infrastructure as it directly translates into lower operational costs while resolving incidents thereby leading to high customer satisfaction.

Scalability: This design factor should be planned for every data centre. It's now a norm to implement load balancing on servers and implement techniques such as reverse proxy caching to offload servers.

Our businesses are no more static, and while most of us find it hard enough to keep track of anticipating future requirements of our businesses from a data perspective, some of us have the additional challenge of identifying and classifying data as "hot" content (such as breaking news stories). While such hot content needs to be identified, data centres should be designed to replicate it to overflow/backup servers or cache to ensure the increased demand is met without compromising performance.

If the data centre is part of a geographically disperse set, then complication will increase greatly. A good design calls for the ability to provide content at multiple sites to allow data to be "closer" to the requesting client, thus providing faster response and indirectly higher availability. Such a design must factor management of data content, synchronization with different sources, distribution of updates, and additional security requirements.

Threats can occur actively or passively from events either outside and inside the data centre itself. We need to ensure that the connectivity paths to external networks, as well as each function inside the data centre (such as gateway or WAN edge, core, distribution and access), are designed with no single point of entry for unauthorized users.

A complete network security solution includes authentication, authorization, data privacy, and perimeter security. Perimeter security is traditionally provided by a firewall, which inspects packets and sessions to determine if they should be transmitted or dropped.

In effect, firewalls have become a single point of network access from which traffic can be analysed and controlled according to parameters such as application, address and user for both incoming traffic from remote users and outgoing traffic to the Internet.

In general, firewalls are intended to protect resources from several kinds of attacks such as passive eavesdropping/packet sniffing, IP address spoofing, port scans, denial-of-service (DoS) attacks, packet injection, and application-layer attack.

It's important to realize that we need to be prepared for ever-changing environments where the kids of today are smarter than most of us and can hack into the U.S. Defence Department with more ease than those of us who struggle to build a PowerPoint presentation on our laptops. ■