Cyber Security: How safe is your building?

A guide to understanding and addressing key cyber risks to your built assets in APAC

Waterstons

CUNDALL

About Cundall
As global multi-disciplinary engineers and sustainability consultants we see how the relationships between people and places can be improved through integrated innovation.

Building controls are part of our core business: we enhance how buildings function and optimise the safety and experience of those who live, work, play and stay in them.

Our teams collaborate across the globe to find ways new and existing buildings, precincts and portfolios can perform better, use less energy, and reduce the impact of our built environment.
www.cundall.com

About Waterstons
For over 25 years, Waterstons has worked side-by-side with organisations across the UK and Australia to solve technology-based problems with innovative solutions.

Headquartered in Sydney, Waterstons is a global company offering completely bespoke technology solutions. Offering end-to-end services with 24/7 solutions across Cyber Security, Technology Consulting, Managed Services, Data & Analytics and more across 4 cities in Australia.

By evaluating people, processes and technology, Waterstons elevates organisations through bespoke and consultative based technology solutions.
www.waterstons.com.au

Contents

01
Executive Summary

> **“It is likely that nearly 40% of BMS (Building Management System) servers in US buildings have been targeted by malware, phishing scams or ransomware.”**
>
> —
>
> US depart of energy

Executive Summary

Connected Buildings: The Next Big Cyber Security Target?

If you've ever asked Siri to turn on some music, waved a digital passcard to access the office on a weekend or used an app to check how much energy your home's solar PV is generating before remotely switching on the air conditioning to cool the house before you get there, you've already experienced some of the benefits of smart buildings and the Internet of Things (IoT).

You will also have seen headlines about the Optus data breach, the Medibank cyberattack and the millions of dollars lost to phishing scams – and may even have been one of the many 1000s of people affected.

Useful as they are, all digital technologies have their own unique vulnerabilities and risks. That includes smart building systems such as controls and automation, IoT devices and cloud platforms used to manage security, lighting, lifts, energy use, air conditioning, ventilation – possibly even the pumps in a building's water supply.

With the heightened awareness of cyber threats, what keeps many asset owners, facility managers and building tenants awake at night is the thought: "What if someone hacks my building?"

There are reasons for concern. A recent report by the US Department of Energy, Challenges and Opportunities to Secure Buildings from Cyber Threats found:

- Almost 50% of US enterprise customers rate security as their primary concern in adopting IoT technologies.
- Around half of all US commercial buildings have devices exposed to the internet.
- 95 percent of sites do NOT have a disaster recovery plan.
- It is likely that nearly 40% of BMS (Building Management System) servers in US buildings have been targeted by malware, phishing scams or ransomware.

Data from the Australian Centre for Cyber Security is also sobering: in the first six months of 2022 an estimated $60 million was lost to cyber scammers and hackers.

Speaking to risks and concerns around smart building technologies and cyber security are at the heart of this eBook. We aim to inform, educate and empower individuals and organisations to gain the benefits of smart buildings and connected devices while protecting themselves and their stakeholders from digital threats.

The ebook has been authored by cyber security and cyber resilience experts from leading digital technology services provider, Waterstons, and smart building and strategic security experts from global multidisciplinary engineering and sustainability advisory firm, Cundall.

Together, we unpack the threat landscape and red-flag vulnerabilities you may not have considered, and explain best practice strategies for protecting people, properties and business operations.

02
How real are the risks?

> **“In effect, cybercriminals are outsourcing elements of their operations, and a growing black market is serving their needs.”**
>
> —
> ACSC

How real are the risks?

Smart buildings and the digital systems that support manufacturing, logistics and critical infrastructure have in recent years become a target for hackers. The Joint Cyber Security Advisory, which includes government agency cyber security experts from the USA, Australia, the UK, New Zealand and Canada has reported that in 2021 the rate of cyberattacks including sophisticated ransomware attacks increased and that it was not only large organisations ('big game' in hacker parlance) in the crosshairs. Medium enterprises in sectors such as food manufacturing or even hospitals have been targeted.

The goal of these attacks is often for financial gain through lockouts on key systems, taking control of critical systems or through threats to disclose stolen data or information to third parties to cause reputational damage or loss of business. In other cases, the aim is to disrupt critical infrastructure operations as part of a broader agenda. A recent example includes cyber attacks linked to Russian operatives targeting organisations that are supporting the Ukraine.

The threat is taken so seriously that in March 2022, US President Joe Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act as a response to high-profile attacks on critical infrastructure providers. The Australian Federal Government also enacted similar legislation in July 2022.

The Australian laws make it mandatory for organisations and businesses in key sectors including energy, communications, food and grocery, hospitals, aviation, freight services, public transport, financial services, higher education, water authorities, ports and Defence industries to report any cyber security incident that poses a significant threat to the reliability, integrity, availability or confidentiality of the asset (or its operations) within 72 hours.

In its 2019 Cyber Security report, Accenture calculated the value at risk from cyberattacks between 2019-2023 at US$5.2 trillion. This calculation was based on the proportion of revenue lost to the financial impact of attacks through damages including business disruption, damage to equipment, loss of crucial data/information, costs of system recovery, payment of ransom demands and legal consequences.

In Australia alone, the Australian Cyber Security Centre's 2020-21 annual Cyber Threat Report noted that nearly 68,000 attacks had been reported over the year, with total self-reported financial losses as a result totalling over AU$33 billion. Approximately a quarter of the reported attacks affected entities associated with critical infrastructure including energy, communications, water supplies and transport. Professional, scientific and technical organisations are also becoming a major target, particularly for ransomware attacks, with the ACSC identifying this sector as the second most frequently attacked. Government agencies are the most frequently targeted by ransomware threats.

The 2021-2022 ACSC annual report showed threats and consequences continue to escalate and evolve. New entities have emerged that provide Cybercrime-as-a-Service (CaaS) and Ransomware-as-a-Service (RaaS). This is enabling individuals and organisations with minimal technical skills or IT infrastructure to commission what they need including servers, bespoke malware, phishing campaigns and money laundering mechanisms.

It is also important to keep in mind that direct attacks on your own organisation or the services you use are not the only risk. Major incidents such as the WannaCry global ransomware attack which began in the morning (UK time) on Friday 12 May 2017 had infected more than 230,000 computers in at least 150 countries within 24 hours, according to Europol. The attack, which exploited an unpatched vulnerability in a legacy Windows operating system - possibly via a Server Message Block (SMB) port - affected organisations including the UK National Health Service, Spain's Telefonica, FedEx, Nissan Motor Manufacturing UK and Renault, where it had infected some production systems.

People often wonder: how easy is it to gain access?

"Scoping the Australian IP Address space, we were quickly able to identify 5,956 Building Management Systems open to the wider internet.

While this does not present an immediate risk, the bigger picture is that there are 5,956 buildings that have their entire management system accessible from anywhere in the world with an internet connection. If just one of those is misconfigured, or is missing vendor security patches, then the entire building's systems can be manipulated from anyone with an internet connection anywhere in the world."

Ryan O'Kell - Waterstons Australia

> **"One cybercrime report is made approximately every seven minutes in Australia."**
>
> Australian Cyber Security Centre (2021-22 annual report)

> **"In effect, cybercriminals are outsourcing elements of their operations, and a growing black market is serving their needs."**
>
> ACSC

03
Smart buildings and connected devices

> **“You cannot secure devices you do not know are connected and potentially vulnerable.”**
>
> —
> US Department of Energy

Smart buildings and connected devices

Overview

Often when media or property sector leaders talk about smart buildings, they paint a picture of brand-new shiny assets with all the technological bells and whistles. The sales pitch often includes mentioning an app that will let someone order their perfect coffee so it is waiting for them when they get to the office and up to the hot desk they booked.

It's the automation and control technology sitting behind the scenes that makes a building operate more efficiently and comfortably. This can include smart lighting systems with occupant sensors that also respond to daylight levels by increasing or reducing brightness levels. The HVAC (heating, ventilation and air conditioning) might incorporate controls and sensors that optimise the level of fresh air intake to maintain excellent indoor air quality and alter the airflow and refrigerant flow to minimise energy use and fine-tune thermal comfort levels.

Access controls are another aspect of buildings that increasingly uses smart approaches including digital pass cards or device-based passes that integrate with destination-controlled lifts, end-of-trip facility access, gym bookings and employee identification verification.

All of these systems can be integrated and coordinated with other elements of building systems or individual items of equipment within an office, retail centre or common area such as smart fridges, smart AV equipment, digital signage, facilities management energy monitoring platforms, the building management system, building automation systems and on-site renewable energy generation and storage technology.

They are not restricted to new buildings either – smart systems are a key tool in the kit for retrofitting buildings to improve energy performance and the occupant experience.

These systems can include networks of IoT-enabled sensors on specific elements of building services such as HVAC air handling units; occupancy/daylight sensors on lighting systems; and submeters for specific electrical circuits. The level of sophistication and degree to which these are coupled with digital building management platforms or building performance analytics software depends on the needs and wants of the asset owner, occupants and the facility manager.

Do you know what's in your building?

In an existing building, one of the challenges can be knowing what has been installed and what systems are operating within or interfacing within it. Buildings change and evolve over time, and individual tenants or facilities managers, building managers or service providers may have introduced smart devices which could create a vulnerability for outside agents to access systems and networks within the building.

Any smart building cyber security strategy therefore needs to incorporate an audit of:

- What systems are in the building (including legacy systems and tenant IoT devices).
- What data is managed by those systems.
- Who has access to those systems.

"You cannot secure devices you do not know are connected and potentially vulnerable."

—

US Department of Energy

04
Retrofit vs new fittings

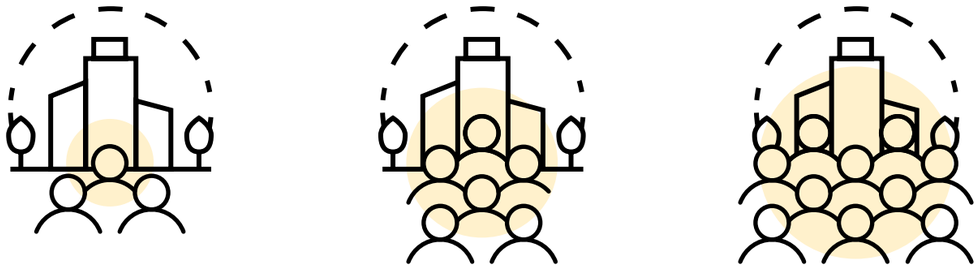
> **“It’s worth noting that malicious actors don’t just want to sit around watching your cameras, hoping to catch you doing something you shouldn’t be. They’re accessing your cameras to infiltrate more important networks.”**
>
> —
> Charlie Hales, Managing Director, Waterstons

Retrofit vs new fittings

Retrofitting your connected building in comparison to retrofitting an older connected building involve quite similar considerations but with separate processes. In both cases the buildings should receive continuous security and system maintenance.

Prior to retrofitting a connected building, a penetration test must be conducted by a third-party entity to evaluate the needs of the building. Then, the needs of the building must be addressed as there may need to be re-cabling, swapping out energy maintenance systems and of course the implementation of new technology, policies and processes. After this time, an additional penetration test should be completed to re-evaluate the effectiveness of the building.

Estimated cost based on ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au.



$39,555
Small business

$88,407
Medium business

$62,233
Large business

Cybercrime reports and average reported loss by organisation for financial year 2021-22

Learn more about penetration testing in the glossary

In a new connected building, Cyber Security should be considered from the early planning stages of the building to allow for the correct technology, electrical cabling and system maintenance to be designed into the building. This is a much more effective strategy than adding smart features as an afterthought. After the completion and commissioning of the building, a thorough third-party penetration test should be conducted to evaluate the effectiveness of controls.

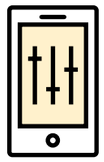
In both cases, Cyber Security in these connected buildings must be a high priority. Maintenance and ongoing security reviews or engaging a dedicated Cyber Security team (depending on the size and complexity of the building) should be implemented to ensure the safety of occupants and the longevity of building systems.

“Phishing campaigns, targeted spear phishing, remote access through vulnerable machines and the use of publicly available exploits remain the most common vectors for deploying ransomware.”

—
Australian Centre for Cyber Security (2021)

What Cyber Security threats could be associated with Smart and Connected buildings?

The rabbit hole of Cyber Security threats is vast and deep and there are not a finite amount of them that can be evaluated. However, this doesn't have to overwhelm you. When creating your Cyber Security roadmap, your third-party Cyber Security contractor will evaluate your business so the solution is completely bespoke and create a plan which mirrors the building's technological landscape. As a general picture of what may need to be addressed, the below threats have been evaluated as most common by the Cyber Security experts at Waterstons Australia and Cundall's Smart Buildings and Security technical leads.



Locks and access controls

Locks and access controls can be bypassed by malicious actors or software which allow or disallow physical access to a building. The scenario could pose as the malicious actor/actors choosing to lock people in or out.

This does not only include technical controls like swipe cards, but can include internal doors, smart elevators and car parks. Swipe cards can be easily cloned and unprotected systems can easily give an adversary the power to take control of elevators and car park areas. Giving them the potential to cause real damage within the building.

How to mitigate the risks:

Access control readers interact with the solenoid door lock, with electronic mortise locks offering better physical protection compared to many other locks. To offer effective security, not only are access control components like locks and card readers etc. are needed, but the entire construction of the space needs to be sturdy. The wall the door is mounted into, the door frame, door, ironmongery and locking furniture comprise the physical security and should be protected from physical attack based on the security risks. Creating a strong physical resistance, with a robust access control system, and procedures such as 2-factor authentication (2FA), anti-pass back through read in and read out help create a holistic defence.

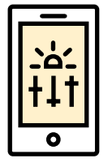
As with all things that are combined from various parts, the weakest part decides how secure the access control or lock system is. What is often left out of the equation is the lock cylinder. If all parts of the lock, along with the actual door, the door frame and the walls, the ceiling and the floor, are up to the highest security standards, there is no point trying to skimp on the lock cylinder, which would then be the weakest link, since a cheap cylinder can easily be picked.

Currently, most swipe cards are of the 125khz RFID type which can easily be hacked and copies can be made within less than a minute using devices that cost less than $20AUD and are readily available over the internet. Unfortunately, many Access Control systems still use proximity cards, which have the advantage of high throughput rate, but very low security. Companies need to move away from this old and unsecure practice and rethink their approach. High security cards are available, and have a throughput rate similar to proximity cards, however, with the disadvantage of higher price. That needs to be balanced however against the financial and other risks if this keeps your premises secure. When using even highly secure credentials, there is always the issue of these credentials being stolen or obtained through social engineering. Anti- can help mitigate part of this risk. . t's always beneficial to have the Access Control System integrated with the Closed Circuit Television (CCTV) System. This way, if a credential gets stolen or if it is willingly handed over to an unauthorised person, when the credential is used to gain access, the system can give an alarm if the face of the user is different from the face of the registered credential holder. One of the attractive options now is to enable mobile access control, and this is getting widely accepted by users. Various technologies can be used to make mobile access safer from hacks and misuse. Naturally, for this to work the IT Department needs to work hand in hand with the Security Department. If a phone gets stolen or is lost, the mobile access function is only then available when the mobile phone is unlocked.

Nowadays, most mobile phones are secured with either PIN or biometric recognition (fingerprint or face). If a mobile phone is lost or stolen, the owner usually realizes this immediately. If an access card is lost, it might take a while for the owner to realize.

Biometric access control methods such as facial recognition, fingerprint recognition, and iris recognition can be used on access doors. Furthermore, implementing a Multifactor Authentication (MFA) system increases security by requiring users to enter a combination of their credentials to gain access.

For locations that need an extra high level of security, the two-man rule is one possible method. The two-man rule involves a protocol where two different persons need to request access, typically using two-factor authentication (2FA), within a very short amount of time, typically within 10-15 seconds. Only when both persons have the correct 2FA credentials and do this within the set amount of time the door will open. Right after entering the room both persons need to verify their presence in the room (after the door has closed) by verifying again with a 2FA they are in the room. Additionally, sensors inside the room will detect how many persons are present. Should there be any more or any less than two persons at the same time an alarm will be sent.



Emergency controls

Emergency controls of the building can be bypassed by malicious actors or software which can prevent the building's technology from correctly mitigating / alarming or reporting emergencies and system failures.

When alerted to an attack, you can safely assume that the adversary has been infiltrating your building and system for weeks, months and perhaps longer. An attacker has already scoped your emergency controls and it's more than likely one of the first things they'll disable. It's their objective to be undetected until their finale.

As these systems are imperative for the safety of a building and those in it and these threats are not outside the realm of possibility, emergency controls must be always protected.

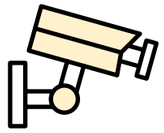
In 2016, a DDoS (Denial of Service) Attack forced the heating devices in two apartment buildings in Finland offline forcing them to get stuck in a reboot loop and leaving residents in the cold until the attack was rectified. Cyber security experts noted that the attack may have been a hacker testing their capabilities to access and disable building control systems in preparation for a much more significant attack.

In 2021, a building automation engineering company lost control of more than three-quarters of the Building Automation Software [BAS] connected devices within a client's building including light switches, motion detectors and shutter controllers after a cyberattack locked it out of the BAS it has built.

Breakout: throughput rate and the benefits of system integration

When it comes to Access Control, one of the issues we need to consider is the throughput rate. When you think of an office with 500 staff, who all want to come to work between the time of 8:50 to 9:00am, this leaves a mere 10 minutes or 600 seconds for everybody to come in, which allows just a bit more than one second per staff member. Even if a building has three entrances, it still means there are roughly just three seconds for each staff member to enter. So considering the efficiency of the access control is vital.

Combining high security proximity cards, mobile-based passcards with MFA in conjunction with other measures can both protect the building and protect the efficiency with which authorised people can enter it. When using even highly secure credentials, there is always the issue of obtaining these credentials by social engineering. What can help here is to apply anti-passback settings in the Access Control System. If a credential gets stolen or is willingly handed over to a non-authorised person, the Access Control System can work in conjunction with the CCTV System, so that through the inbuilt AI in the camera the user of the credential can be compared to the holder of the credential to have a visual confirmation.



Security camera management

Nowadays, security cameras are IP based, which means, they run on a network. If these security cameras are not properly secured they could potentially be accessed, allowing an adversary to view people, systems and processes. For example, a malicious actor could enter the system and watch people type in passwords, monitor movements and behaviours to understand internal process and potentially exploit that information. Adversaries could also tamper with footage, deleting footage or even stopping it from recording.

A scenario arising from this could be a malicious actor stealing certain footage/audio to blackmail the company they have stolen it from and ask for ransom in exchange for not leaking sensitive information. However, most attacks on CCTV cameras are generally an attempt to access to the wider network.

To mitigate this risk, all security systems should be hosted on one platform, so instead of securing every individual system separately such as access controls, CCTV etc, it is the platform that is secured which then ensures all systems on the platform are also.

Additionally, access to any and all network ports, for example where IP network cameras are plugged in, needs to be prevented and/or secured. When outsiders get access to the network, for example through the network cables in the meeting rooms, ensure there cannot be any access to the internal network through these ports. There is also a human defence layer to consider, for example company policies specifying no outsiders are permitted in meeting rooms unless they are accompanied by company staff.

Networking segregation is vital to your protection. Not only do your IT/Cyber teams need to ensure your network connections to the internet are protected, they also need to ensure all your systems like HVAC, security cameras etc are separate entities with blocked network ports. This is similar to the way in a suburb where all the houses may be on the same street - but each driveway has an individual gate. Access to CCTV footage, either live or recordings on servers, should be password protected, preferably with 2FA protection. Tampering with footage and deleting footage should be made impossible, for both insiders and outsiders alike.

> **"In this case, building management firms had a large volume of the BMS' they manage hacked and were locked out with the systems now in the hacker's control. All the buildings affected had to revert to manually flipping on and off central circuit breakers in order to power lights in the building. The devices were ultimately 'bricked', meaning they were destroyed and inoperable via software."**
>
> Ryan O'Kell, Waterstons Australia

> **"It's worth noting that malicious actors don't just want to sit around watching your cameras, hoping to catch you doing something you shouldn't be. They're accessing your cameras to infiltrate more important networks."**
>
> Charlie Hales, Managing Director, Waterstons

Building management system security

The BMS is the equivalent of a nervous system for building, and in most smart buildings has integration with all building services including lighting, electrical, water, lifts, access systems, ventilation and air conditioning. Increasingly the hard-wired systems connected to the BMS using an IoT architecture that facilitates remote access and monitoring of building services by facilities managers, asset managers and relevant third parties. Cloud-hosted BMS systems are particularly useful where a building is being retrofitted for improvements to energy efficiency, indoor air quality and an optimised occupant experience.

With the benefits, however, come the risks of cyber attackers gaining access to other building systems via a poorly-secured BMS. To reduce vulnerability, a BMS platform can be secured via adding more layers to access the system. The popular way is to enable Single Sign On through the corporate multifactor authentication.

However, the popular way is no longer sufficient protection. Network segregation is the vital component to ensuring your critical systems are protected. For example, if an adversary infiltrates your CCTV, network segregation ensures they can't then access your BMS or critical data.

In addition, in order to access the BMS system, any changes to critical systems (such as electrical, ventilation or vertical transportation) requires another set of different user level permissions and a separate password. For devices such as on-site desktop computers of building manager/ facilities manager laptops or iPads, the password saving option should be disabled, including blocking pop-ups that ask the user to save the password in browsers.

Network and server hardening will also provide highly secure network and computer access, lowering the risk of vulnerabilities. This includes changing default credentials and IP addresses, disabling default configuration and rules, creating role-based user accounts with strong passwords, enabling session timeout, shutting unused ports and making regular backups.

Considering the network configuration, the system manager or system designer can enable intrusion detection system (IDS), activate port security by MAC address and implement an Access Control List (ACL) to help ensure a more secure BMS network.

Modern intrusions on a PC or Server aren't typically detected in the same way a virus may have been previously. In the past, Anti-Virus scanners would search for malicious software, flag and remove it. However, with advanced threats comes advanced tooling and this is where EDR steps in.

EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response) are two cutting edge detection and response systems which all devices parallel to a BMS should have.

EDR monitors the behaviour of your PC as opposed to just the files themselves. This includes network connections, how programs are interacting with each other and the files on the system. Based on behaviour, if your PC or server is reaching out to known malicious IP addresses or if a piece of software is accessing something it shouldn't, for example cached passwords, not only are alerts thrown for deep investigation, but a response is also put in place. This could include restricting the machine from accessing the internet or halting a program from performing a specific activity.

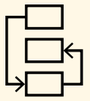
Given the depth of analysis, EDR systems are known for extremely deep event logging, in many cases, better than the system logs themselves, enabling great investigation capability.

Top tips from smart building experts

Tips for smart buildings that apply for all IoT or any devices connected to the internet

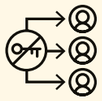
An IT protocol can utilise or create the time period profile login for each user based on regular working hours.

Don't connect the BMS-related IP devices directly to the internet, Always use a firewall to connect to the BMS system from the internet, and in a firewall ensure the particular ports are only enabled.



Use the network traffic monitor software to monitor the amount of data flow.

Do the penetration test often on the BMS network and server.



Disable multiuser login with the same user account.

Linux OS is safer, for very sensitive projects, it is better to use the Linux-based IP devices and OS.

A modern network however isn't just comprised of PCs and Servers. This is especially true of BMS networks. The devices may be running any number of embedded systems and in this case, you would want an XDR (Extended Detection and Response) solution to monitor these devices.

XDR tools come in many shapes and sizes, in some cases bundled with EDR. In others, separated devices that sit on the edge between your internal network and the internet. The gap XDR aims to fill is the ability to monitor the activities of devices that can't be monitored by installing some software. This can include phones, printers, surveillance cameras, network attached storage etc. In this case, XDR can help identify when systems are performing strange actions, for example reaching out to external networks they have never communicated with before, or touching internal systems they have no reason to touch. Think of a camera attempting to log into your BMS web platform.

While EDR offers a great visibility over your devices and the behaviours they exhibit, XDR allows wider monitoring and response capabilities to your network.

You might wonder - How do we protect the delivery supply chain of connected buildings?

The manufacturers of the software used to manage the building and the hardware put in place need to be vetted based on your organisation's threat profile. For example, if we are talking about a government agency, you'll probably only want devices that are manufactured locally or in an approved country by organisations that have certain Cyber Security controls in place.

For example, do they have a security team, do they have their hardware/software tested regularly, do they have vulnerability management, do they have a CISO (Chief Information Security Officer), do they do patch management, how long do they support hardware/software with security updates, do they have a bug bounty program, do they have any relevant qualifications, certifications or credentials like ISO27001, NIST, ASD E8, Cyber Essentials?

Top tips for a more secure BMS system

Where a new BMS is to be installed, there are some strategic ways to design a more secure system for the IP network installation

Only used managed switches with appropriate management software.

Network Segregation.

XDR and/or EDR Systems.

Ensure IP addresses for any device connecting to the network are kept completely private and secure except for when needed to do the configuration.

Ensure spare ports on managed switches are also physically blocked with port blockers.

Ensure third party devices connecting to the network (eg. HVAC chillers, Variable Speed drives on pumps etc.) do not have additional spare IP ports.

Consider implementing a 'device qualification process' where only approved devices can connect to the IP network - these are devices that will have undergone a cyber security test prior to being supplied for use to customers.

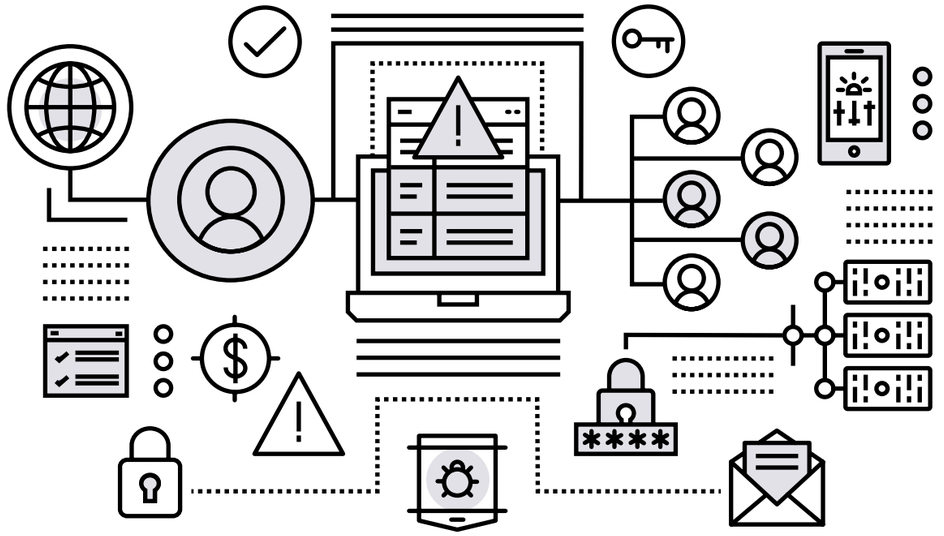
05
The human element

> **In the same way an attacker would target common software that is poorly prepared, they are also looking to poorly prepared people and internal process to grant them access.**
>
> —
>
> Ryan O'Kell, Head of Cyber Security, Waterstons Australia

The human element

When most people think of cyber security they think of antivirus software, firewalls and other digital architecture that protects an individual device and the networks it is connected to from threats including viruses, trojans and other malicious code-based attacks.

The first line of defence is, however, your people. The most common forms of cyberattack attempt to exploit the vulnerabilities of humans to gain access to information and digital systems.



Phishing attacks, for example, are a frequent occurrence. They often take the form of an email or text message with links that purports to be from someone within an organisation, a potential customer, a government agency or a service provider. The goal of a phishing attack is to make the recipient enable access, for example by entering information that then gains the hacker access to personal or company information, or to encourage clicking on a link or opening an attachment that contains malicious code.

According to the Australian Competition and Consumer Commission's Scamwatch, Australia lost a record $323,700,000 in 2021 to scams and phishing which is an 84% increase from 2020. This record growth is exemplary of not only the growth of these scams in both sophistication and volume, but also their ability to dupe average Australians.

We've all been there, someone's holding a million coffees and they shout out "Hold the lift!" or "I can't reach my swipe key, can you swipe me in?" Instinctively and trustingly, we do. When operating in a large building, it's near impossible to keep track of everyone who works in said building but it is the responsibility of each individual to double check swipe passes and authorisation. It's easier than you think to infiltrate a building, go undetected, scope it out and plan an attack from there.

How can we prevent these attacks?

Social engineering (SE) is basically tricking someone into believing you are someone you are not or have authority that you don't possess and then using that illusion to have them give you access to something. Phishing or scam emails are a common form of SE.

Insider threats are another human element to consider. For example, Employee A has been let go due to HR complaints and they believe this was unfair, and they also have the ability and the access to cause damage. They might, for example, steal information, data or reports and sell it to competitors. Or they may use social media to damage the brand reputation or use stolen information to undermine key stakeholder relationships.

In some cases, internal threats are not acting with malice aforethought. They may just be negligent - or sometimes incompetent - and manage to cause harm through a lack of understanding of the consequences of their actions. Think Employee B deleting all the emails in a shared mailbox, opening a phishing e-mail, or being tricked into buying gift cards for their fake boss.

Other forms of social engineering include: fake calls of persons impersonating a superior and demanding information on a very short notice, or a malign actor friends somebody over social media and spies out their likes and dislikes, potentially finding somebody who might be disgruntled with their employer.

The possibilities for social engineering are endless and can only be countered by awareness through training and by adhering to company procedures to minimise the risk of information being given to the wrong person.

> **"Adversaries will enter a building, potentially leave something, take something away or even plant a trap. This could be a USB for example that says 'Payroll'. A curious and unsuspecting individual will plug it in and there lies an easy access point for them."**
>
> —
>
> Charlie Hales, Managing Director, Waterstons

> **"In the same way an attacker would target common software that is poorly prepared, they are also looking to poorly prepared people and internal process to grant them access. Be it through social engineering/phishing or taking advantage of a disgruntled employee, cyber security is an arms race with people presenting as a common weakness in every organisation."**
>
> —
>
> Ryan O'Kell, Head of Cyber Security, Waterstons Australia

06
How to turn human risks into human shields

> **“Cyber security should be the first consideration when designing a digital building platform. In fact, creating a cyber-security policy and program, before selecting any hardware or software providers, should be the priority.”**
>
> Annie Nguyen, Associate, Cundall

How to turn human risks into human shields

Effective training and clearly communicated company policies that explicitly address key risks is a vital part of any cyber security strategy. This could span across even your social media, BYOD policies and physical safety protocols. Ensuring you also have appropriate settings for company devices or for accessing company data and systems via personal devices is also important.

Zero Trust policies

One way to increase the resiliency of security and cyber security systems is a "zero trust" policy. This means a security framework which requires all users to be authenticated, authorised, and continuously validated for security configuration and posture before being granted access to applications and data. It applies to anybody who applies for access, inside or outside the organisation's network.

This can also be expanded not only to users, but to any and all equipment being used within the network, no matter how big or small the equipment is or what the potential use within the network. Having 100% of equipment and users authenticated, authorised, and continuously validated increases the resilience of the systems.

Zero trust policies may seem like an unfriendly concept, but it's simple. Continual validation and up-skilling is an effective way to ensure your organisation is secure. A mix of technologies and processes can be applied. This can include MFA/2FA, Online Upskilling Certificates and tech like Bit Locker and Kerberos.

People often wonder: Is it better to have staff using company devices or BYOD (Bring Your Own Device)?

Company devices are easier to manage and introduce less security risk, assuming your internal IT department and Cyber Security department have the capability to provide each member of the organisation with devices. Having company devices creates a tighter belt around Cyber Security and ensures company-wide protocols and systems are in place for greater protection.

BYOD is certainly an option, and in this hybrid working era, staff may often need to use their own laptop, smart phone, tablet or desktop to carry out some of their work. Keep in mind, managing remote access and BYOD devices within the wider organisation's network can often mean more work for your internal IT department, but with the right team and protocols, it can be just as effective.

One of the most important protocols to have in place for BYOD and for any remote connection to company servers is device compliance which includes up to date software and antivirus and accessing via MFA.

This thought can be extended to USBs. Swapping USBs from work to personal computers can be challenging to manage. It is recommended that organisations who require their people to use a USB should be issued one from the organisation itself, used on its devices and not on personal devices and they should be managed and encrypted effectively.

What is MFA and how does it work?

Multi-factor authentication is a system that requires more than one type of authentication for someone to be able to access something. For example, your e-mails or other accounts.

It works by logging into an account, for example, your e-mails with your normal password. Your authenticator account or application will prompt you to input a second round of data to ensure that the person attempting to access said account is really you. This might be a code you need to enter that has been sent to the mobile phone registered to your account, or to a second email address also registered to the account. Some MFA systems also use an app on the phone connected to an account and the user must manually authenticate the log-in via the app.

MFA is rapidly becoming standard practice not only within businesses but also for government platforms such as the Australian Government's MyGov platform, which requires MFA for every log in.

People often wonder – is it OK if my staff use public WiFi?

Yes, relatively. However, always double check with the venue or signs advertising the WiFi credentials. Most organisations that host public WiFi will have processes in place to stop people connected to the WiFi from contacting each other's devices, but this should not always be assumed.

Best practice is to always use a VPN (Virtual Private Network) and ensure your device's software and antivirus protection is up to date. It is recommended by Cyber Security professionals to avoid public Wi-Fi where possible and use your personal data if you have the capacity.

It's also worth noting that adversaries have been known to create fake public Wi-Fi in order to gain access to unsuspecting devices.

Why should people use VPNs?

Using a VPN is important as it ensures that all your traffic is hidden from view to any potential ‘eavesdroppers’ on the network you’re using. For example, if you’re using public WiFi and a person can access your device, they might be inclined to not only snoop around your device but breach some of your data.

The face of smart buildings - Facilities Managers

Facilities Managers and their staff sit at the nexus of smart systems, the building, building occupants and those service providers and others who have reason to be in a building and potentially access its systems.

This also means they are a key line of defence for preventing cyberattacks and hacker activities.

One of the main threats to watch out for is pretexting - a social engineering attack where an individual pretends to have reasonable cause to access the building or a building system either in-person or virtually.

What to do:

- For an email-based access request - check credentials and email veracity as you would any other potential phishing email. For example, if you receive an email that claims to need urgent access to remotely test an aspect of the BMS or a building service connected to the BMS, do not click anything. Check the claim by calling your usual point of contact for that organisation - and if you have not heard of the organisation before, call your leasing agent and ask them to check.
- For an in-person visitor - ask to see credentials including both their head office number and their personal mobile number. If the visit is unscheduled and you did not call for a service provider, enact a Zero Trust approach - check the company has a website and call to verify identity using the website contact number.

To secure the BMS against digital cyberattacks:

- Keep antivirus and windows up to date (you would be surprised how often this is not done).
- Change passwords frequently (you would be surprised how often they are never changed from something like Admin123).

“Cyber security should be the first consideration when designing a digital building platform. In fact, creating a cyber-security policy and program, before selecting any hardware or software providers, should be the priority.”

—

Annie Nguyen, Associate, Cundall

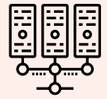
In summary - 10 top takeaways

Always use a firewall to connect a BMS system from the internet, and in a firewall ensure the particular ports only are enabled.

VXDR (Extended Detection and Response).

Ensure complex password policy is enforced in the vendor products/system.

If any employee resigns, de-activate his/her/their account immediately.



Use network traffic monitor software to monitor the amount of data flow, particularly video files - set the system to raise an alert if any abnormal activity happens.

Network segregation.

Disable multi-user login with the same user account.

Practice security convergence.

Maintain a dedicated security network.

Have a zero trust policy.

Undertake staff awareness and training.

Be alert for social engineering.

07
Prevention and risk management

> **All organisations need to prioritise excellent Cyber Security practices to ensure they even qualify for insurance. We're going to see a lot of companies not being eligible for insurance because they're simply not Cyber Safe enough.**
>
> Charlie Hales, Managing Director, Waterstons

Prevention and risk management

Why security integration matters

The ISO/IEC 27032 standard for Cyber Security is the global benchmark for integrated security approaches. It covers all the bases from the physical asset and human vulnerabilities through to digital systems such as protection to manage Cyber Security risks, implement security controls, incident response and security awareness.

When it comes to cyberattacks, we must not only look at the individual systems within the realm of Security systems, but at the platform on which all Security systems are hosted. Modern platforms have a very strong stance on securing the platform against all kinds of cyberattacks, which is, of course, an absolute must.

Another best practice is to have a network exclusively dedicated to Security use. The IT Department needs to have the relevant security for the dedicated Security network in place, i.e a firewall.

But thinking in single systems and kits of parts is not optimal. Keeping smart buildings safe requires Security Convergence - the merging of the IT Security and the Physical Security Departments.

Nowadays, all Security systems run on software and hardware, which means there is a lot of equipment needed for Physical Security that also needs to tie into the IT setup and therefore into the IT Security. Up until very recently, the approach for IT Security and Physical Security was to each be in their own "silo", which is why people often talk about the "silo mentality".

But with the rise of cyber threats we can no longer afford to think and act in these silos, which is why Security Convergence is essential. It will help make the Security platform and all systems on it much more resilient to cyberattacks.

“Protecting the gateway to an organisation, building, asset, or individual system requires physical security, electronic security, cyber security and controls. Firewalls at service providers and security controls, DMZs on building systems, up to date software, authentication systems and constant updates provide a holistic solution to stop threats at source.”

—

Stephen Fry-Harris, Associate Director, IT and AV, Cundall.

Government tenders and requirements

In Australia, many Government Tenders are asking businesses to be Essential 8, ISO27001 or NIST compliant in order to apply for consideration. This new trend is almost exclusive to Government Tenders and is yet to be adopted across all industries and sectors.

Comparing Australia to other countries, particularly Europe, we are falling behind in our requirements for cyber safety. You only have to glance at the daily headlines to see news outlets, radio, and TV news reporting on major breaches affecting millions of Australians. The Essential 8 is the current Australian accepted standard and Cyber Security experts believe it should become the industry standard across all industries and sectors.

At a minimum, connected buildings should aim to be Essential 8 compliant. Being Essential 8 compliant provides companies a clearer pathway to cyber safety and a minimum protocol to abide by. Cyber Security experts do strongly recommend being compliant in Essential 8 and we believe adopting this minimum protocol will increasingly be a necessity in the near future.

Insurance

Following on from the previous statements regarding minimum compliances, the trend of insurance companies requiring organisations to be either Essential 8 compliant, a penetration test from a 3rd party or another measure of Cyber Security compliance is on the rise.

The metaphorical belt of insurers is tightening when it comes to Cyber Security as organisations are becoming uninsurable due to their lack of compliance or their unwillingness to comply. Similarly, this trend of insurance companies requiring organisations to be Cyber compliant in some capacity will only increase.

> “Insurers need to, and do, take steps to assess the risk being underwritten in a cyber insurance policy. This process involves assessing the likelihood of an attack on any company, which requires access to reliable cyber incident data, and the likelihood that such an attack would impact the policyholder. To do this, insurers need to make an assessment of any risk mitigants, such as, the company’s cyber security controls to price the risk they would assume in writing the policy.”
>
> **Insurance Council of Australia**

“All organisations need to prioritise excellent Cyber Security practices to ensure they even qualify for insurance. We’re going to see a lot of companies not being eligible for insurance because they’re simply not Cyber Safe enough. You wouldn’t expect your car to be insured for theft when you never lock it. It’s the same concept.”

—

Charlie Hales, Managing Director, Waterstons

Critical steps to a safer smart building

Penetration testing

Incorporating regular penetration testing by third party Cyber Security organisations is an essential way to ensure that as your systems change, you're always aware of the holes in your systems and what needs to be changed in order to stay protected.

However, there are many ways penetration testing can be performed. For building maintenance, you are likely to want to have someone test your security guarding, the building access controls and any additional technology that is unique to your building.

Cyber security planning

All the above can be difficult and overwhelming to manage and keep on track with. Employing a great third-party Cyber Security team either remote or on site to manage all things Cyber Security is one of the best ways to protect your organisation for the long term.

It's unlikely that your internal IT team or managed services provider can complete these tasks in full, although general IT teams are experts in their field. But Cyber Security is almost an entirely different ball game. You wouldn't hire a plumber to do electrical work on a building, would you?

Your dedicated Cyber Security support should not only advise you on the best strategy for long term maintenance, create that strategy and implement it but guide you on trends in the market and innovate and adapt with the latest Cyber Security protocols and requirements.

This team should not only be an afterthought post-build when considering a new building. They should be part of the inception stage, when designing and engineering the building. They can help answer complex technical questions like what technology will go into that building? Why is one technology safer than the other?

A Cyber Security contractor on your team can result in economic savings during inception and also down the line once the building is completed. They can also provide guidance to ensure excellent records are kept, the Cyber Security maintenance team have a well reported clean slate to manage.

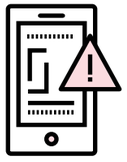
Penetration Testing

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. It is often used to identify vulnerabilities in a system that could be exploited by hackers, and to assess the effectiveness of the system's security measures. In the construction industry, penetration testing could be used to evaluate the security of a company's computer network, for example, to ensure that sensitive information about projects and clients is protected from unauthorised access. Just like a building inspector might check the structural integrity of a building, a penetration tester would evaluate the security of a computer network to ensure that it is secure and able to protect against potential threats.

Cyber security hygiene

Cyber Security Hygiene is a set of practices put in place to ensure organisations, their people and their assets are adequately secured from attacks.

This is typically just good practice encompassing patching, password controls, cataloguing IT software and hardware and inventory and monitoring your catalogue for changes or new vulnerabilities. Good cyber security typically stems from good network administration and best practice, Cyber Security Hygiene is making sure this is done right.



Ramifications of threats

Considering all the above, you've evaluated your risks, created an excellent plan and are now compliant to the highest degree of Cyber Security, your risks are minimal, and your people, processes and overall organisation are protected. What could be some consequences to ignoring all the above?

Many of the consequences below overlap and go hand in hand. However, they're all just as important and are all just as real as one another.

Mini Case Study: Optus Breach - We Trusted You

Each breach comes with undeniable and varying consequences. However, the Optus breach personified each and every consequence imaginable for an organisation. From a PR disaster to safety to class actions, this breach is one of the most significant in Australia's history.

The quote 'sophisticated attack' was inflicted on 7.7million Australians and over 10,000 Aussies had their data leaked by the 'OptusData' alias on the Dark Web. The organisation was exposed and vulnerable through un-encrypted data which was exploited by 'OptusData'. This attack wasn't necessarily 'sophisticated', the adversary just knew where to look. This hacker even went as far to say online "No authenticate needed. That is bad access control. All open to internet for any one to use."

Optus has been a household name in Australia for decades and millions of people trust Optus with their business devices, their children's first mobile phone and most importantly - their personal data. They've certainly lost the trust of many individuals and organisations across the country with such a preventable breach.

They say all publicity is good publicity. However, when your organisation is front and centre after a Cyber Security breach and the public now distrusts your brand, it's hard to imagine the publicity was beneficial. The onslaught of negative publicity Optus has received has certainly obliterated brand credibility which takes years, if not decades to replace. The brand is no longer first thought of as a national Internet Service Provider (ISP) who provides a range of accessible services but simply, a Cyber Security breach.

Individuals have taken to Facebook to express their anger over the breach saying; "Absolutely disgusting, you are vetting and deleting comments." and "This company can't be trusted.". This is a mere snapshot of the thousands of conversations families are having about their data being breached.

Amongst these conversations are actions, with Optus losing over 10% of their current customers and is likely to translate into a decrease of overall profits. Despite their share prices taking a dive during the days and weeks after the breach, the share price has steadily been increasing. This could be taken as a win. However, with class actions looming and contracts to be renewed from current customers the full effect of the breach will not be felt for years to come.

The near future is likely to involve Optus seeing class action lawsuits sent to their legal teams (which are already underway), their teams will have to be held accountable to legislation and will be facing some hefty fines from the Albanese Government worth millions.

This mini-case study illustrates the depth and breadth of complex multi-faceted consequences that could be potentially faced by organisations who don't prioritise Cyber Security. The technical component of Cyber Security may seem overwhelming, time consuming and complicated. However, it's not the tech you need to know. It's the risks your organisation faces and the consequences that may result which you really need to be across.

Loss of profits and/or revenue

All too often, Cyber Security is seen as an afterthought for organisations, until they're breached and then to fix said breach can sometimes cost hundreds of thousands of dollars. Tougher penalties have been seriously discussed in parliament by the Albanese Government, and it would be wise not to call their bluff. These breaches result in a loss of profit and revenue as the business stops operation, pays large amounts to fix the issue (in a lot of cases, we see organisations not retrieve all breached information), potentially install new software/hardware, all whilst paying the running costs of the organisation.

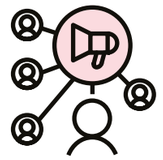
Not only are these upfront costs involved, what also needs to be factored in are the long-term costs; such as a public relations and marketing damage control, potential fines, lawsuits (if personal information is breached) and the credibility of the business being compromised which may affect future deals.

Loss of productivity

If an organisation is breached, what must be considered is the business may need to cease operations, and employee's may need to stop their work. This could mean productivity loss for the foreseeable future.

This un-planned loss of productivity could also manifest itself as additional training for all employees of the organisations in Cyber Security. Sometimes, this training could take days or weeks to complete, halting productivity in the workplace.

For example, Company A has great Cyber Security practices whereas Company B doesn't. An adversary has infiltrated both companies. Company B begins to flounder as their people, processes and technology are compromised. Company A reaps the rewards.



PR disasters and brand erosion - loss of trust

The last thing any organisation wants is a public relations disaster. You've been breached, the press has gotten hold of the story, the company is portrayed as negligent, non-compliant and your public relations team is working overtime to squash the story. However, Cyber Security continues to be a hot topic for the press, and it snowballs.

Where does that leave your organisation? You're either employing a PR company to clean up the mess whilst your revenue potentially plummets as your credibility and market share crash amongst clients and the public.

"I've personally seen organisations decimated by breaches. The lack of adequate Cyber Security and the subsequent consequence they inherit sends them to the brink of no return. Damage can be irreparable and not only are profits lost or there's bad PR. You simply lose your brand and business. It's not worth losing your business over something so simple to implement."

—

Charlie Hales, Managing Director, Waterstons

Potential government fines and prosecution / lawsuits

There are a range of regulations around cyber crime and cyber risks that organisations need to be aware of, as some of them impose obligations on potential targets. Data breach regulations that have been added under Australia's Federal Privacy Act (1988) for example make it mandatory for any organisation whose activities fall under the Act to report any incident where personal information is accessed or lost.

This effectively means that customer contact and account information, human resources records on employees, payroll information and banking details, workplace health and safety incident reports - even internal emails and documents are all potentially data covered by the regulations.

These are also areas of an organisation's activities that are attractive to hackers, as has been seen with multiple recent cyber-attack incidents including the 2021 incident when the personal details of approximately 80,000 South Australian government employees were stolen in a data breach.

Safety

The responsibility to keep people safe in your buildings is ultimately the top priority. If an adversary were to penetrate systems, lock everyone inside for ransom and manipulate your HVAC systems, lock people inside elevators for ransom or worse, the responsibility falls on those who own and operate the building. This may seem in the realm of impossible, but it has happened before and has the potential to happen again.

For example, a hotel in Austria was subjected to ransomware attacks four times between 2016 and 2017. The hackers exploited a vulnerability in the hotel's digital door key system and locked guests out of all rooms - and also locked up parts of the hotel's business management system and equipment. The hotel management paid the bitcoin ransom the first time, so the attackers circled back and did the same thing again... and again... until management brought in cyber security experts and addressed the flaws in its systems.

A cautionary tale: Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883

- Pouyan Aski, Senior Electrical Engineer, Cundall & John Van de Poll, Partner & National Insurance Team Leader, Holman Webb Lawyers

Insurance against loss or damage caused by cyberattacks is important, but keep in mind it may not cover all the costs associated with mitigating and recovering from an attack. Nor will it necessarily protect a company bottom line from loss of business income due to an attack.

For example, the 1 August decision of Federal Court of Australia in Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883, considered the expression "Direct Financial Loss.... directly caused by" for the purposes of first-party coverage under cyber insurance policy.

Facts of the case

The Plaintiff in Limited v Chubb Insurance Australia Limited [2022] FCA 883, Inchcape Australia Limited ("the Plaintiff") claimed that they must be indemnified for an amount of up to $2.3 million for a "ransomware attack" on its computer system under a Financial Institutions Electronic and Computer Crime Policy ("Policy").

The Plaintiff claimed that a ransomware attack encrypted its primary server and offsite backups, deployed malicious software to laptops and desktop computers, and copied data from a shared drive and published it on the dark web.

The Plaintiff claimed that the ransomware attack caused it to incur, and continued to incur, financial losses in repairing and/or replacing hardware, software and data, including investigation costs, hardware costs, resources costs, additional staffing costs, and data recovery costs.

Read the full legal case review and what the court decided in Appendix A

08
Cyber security trends and predictions

> **“Cybersecurity authorities in the US, Australia and the UK assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent.”**
>
> —
> Australian Cyber Security Centre

Cyber security trends and predictions

As more systems continue to be connected to the internet every day, the opportunities for malicious actors become an endless well of vulnerabilities to exploit. Cyber Security systems in connected buildings should never be 'set and forget'.

There are a multitude of these systems out there which are not maintained or even on the radar of internal IT and security teams. Without visibility or consideration here, a new attack vector is being created each time a building is becoming connected whether it be retrofitted with new technology or a new building entirely.

Predictions from the Cyber Security Experts at Waterstons Australia are not new to the market. Cyber Security threats are on the rise and continue to and yet the care and maintenance to protect individuals and organisations are not being taken seriously enough. For organisations today it isn't if you will be attacked but when.

The vast majority of Cyber Crime is opportunistic as opposed to sophisticated. Finding and exploiting security holes is trivial - not getting caught is the hard part and with attackers finding safe harbour overseas, the hard part of hacking is removed. As a result, we're seeing a constant evolution of the opportunistic attacks being carried out. The bottom line is a vast majority of the internet is insecure and vulnerable to attack, it's just a matter of adversaries finding and exploiting new attack vectors. In the case of Building Management Systems, there are hundreds of thousands of these devices sitting open to the entire internet, many have default credentials, many more haven't been updated since they were installed and are now vulnerable. While ransomware is big on everyone's minds, it's only a matter of time before these attackers broaden their focus to include BMS/ICS.

"Cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model."

—

Australian Cyber Security Centre

"Over the last two decades we have seen a parabolic increase in technology use, however it has only been the last 5-10 years we have started to put an emphasis on the security of this technology. As a result we have inadvertently stood up billions of devices, many vulnerable and misconfigured and we have connected them all together via the Internet. Day by day more technology is brought online, more software is built, more vulnerabilities are discovered, more attackers build ability and as ability imparts on ability we will only see this problem grow. This problem isn't a new one, it's just one we are only starting to see impact from and as an industry, we're just starting to catch up."

Ryan O'Kell

"This isn't simply the responsibility of IT and Cyber Security Experts anymore. Cyber Security and data protection is the innate responsibility of Boards, Directors and frankly - everyone in the organisation. It's no longer an 'if' but 'when'. With tougher penalties and a barrage of attacks on the horizon, this isn't an issue that will disappear - quite the opposite. We're going to see a lot of Cyber Security companies grow in the coming months and years, that's for sure."

—

Charlie Hales, Managing Director, Waterstons

09
Conclusion

Conclusion

Every asset owner, asset manager and building occupant needs to understand and act on cyber security. The potential risks associated with the adoption of smart building technologies and the use of the Internet of Things (IoT) are significant and should be carefully considered by organisations in all industries. The information and strategies presented in this ebook provide valuable guidance for organisations seeking to secure their systems and protect themselves from the potential impacts of cyber attacks.

By understanding the threat landscape and implementing best practices for securing their systems, organisations can gain the benefits of smart building technologies while minimising their exposure to risks. This is particularly important given the increasing reliance of businesses and critical infrastructure on these technologies, and the potential for significant financial and reputational damage that can result from successful cyber attacks.

Appendix A

A cautionary tale: Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883

- Pouyan Aski, Senior Electrical Engineer, Cundall & John Van de Poll, Partner & National Insurance Team Leader, Holman Webb Lawyers

Insurance against loss or damage caused by cyberattacks is important, but keep in mind it may not cover all the costs associated with mitigating and recovering from an attack. Nor will it necessarily protect a company bottom line from loss of business income due to an attack.

For example, the 1 August decision of Federal Court of Australia in Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883, considered the expression "Direct Financial Loss.... directly caused by" for the purposes of first-party coverage under cyber insurance policy.

Facts of the case:
The Plaintiff in Limited v Chubb Insurance Australia Limited [2022] FCA 883, Inchcape Australia Limited ("the Plaintiff") claimed that they must be indemnified for an amount of up to $2.3 million for a "ransomware attack" on its computer system under a Financial Institutions Electronic and Computer Crime Policy ("Policy").

The Plaintiff claimed that a ransomware attack encrypted its primary server and offsite backups, deployed malicious software to laptops and desktop computers, and copied data from a shared drive and published it on the dark web.

The Plaintiff claimed that the ransomware attack caused it to incur, and continued to incur, financial losses in repairing and/or replacing hardware, software and data, including investigation costs, hardware costs, resources costs, additional staffing costs, and data recovery costs.

The Plaintiff relied upon the Policy pursuant to the following insuring clauses under Insurance Agreement 2 ("IA 2"), and Insurance Agreement 3 ("IA 3"):

1. Computer Virus (IA2): Direct Financial Loss by reason of the loss resulting directly from the damage or destruction of Electronic Data, Electronic Media or Electronic Instruction owned by the Insured or for which the Insured is legally liable while stored within a Computer System covered under Insuring Agreement 1 ("IA 1")

2. Direct Financial Loss resulting directly from:

   a. The fraudulent modification of Electronic Data, Electronic Media or Electronic Instruction being stored within or being run within any system covered under IA1,
   b. Robbery, burglary, larceny or theft of Electronic Data, Electronic Media or Electronic Instruction, or
   c. The acts of a hacker causing damage or destruction of Electronic Data, Electronic Media or Electronic Instruction owned by the Insured or for which the Insured is legally liable while stored within a Computer System covered under IA1.

The Defendant in Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883, Chubb Insurance Australia Limited ("the Defendant") contended that there was no cover for Repair and Replacement Financial Losses under IA 2 and IA 3 because:

1. There can be no indemnity under IA 2 and IA 3 the "Direct Financial Loss ...covered under IA 1" is satisfied ("Contention 1").

2. The indemnity under IA 2 and IA 3 is confined to the cost of actually reproducing damaged or destroyed Electronic Data, Electronic Media or Electronic Instruction by operation of general condition 4(i) and will not extend to the additional costs incurred if such data is actually reproduced by other Electronic Data, Electronic Media or Electronic Instruction of the same kind of quality ("Contention 2").

3. Consequential or indirect or insufficient direct losses for the purposes of IA 2 and IA 3 are excluded under the Policy ("Contention 3").

The Decision
Firstly, for Contention 1, the Court concluded that so long as the Computer System is covered under IA 1, the indemnity cover under IA 2 and IA 3 will be available.

Secondly, for Contention 2, the Court held that the correct question is "whether the cover available under IA 2 and IA 3 is limited to the cost of the blank media plus the cost of labour for the actual transcription or copying of data if such Electronic Data (etc) is actually reproduced by other Electronic Data (etc) of the same kind of quality" and not the question of "direct financial loss resulting from".

Thirdly, for Contention 3, the Court held that the cover is for "Direct Financial Loss" "resulting directly from", the proximate cause of which is an insured event. Her Honour held that the cover is not for Direct Financial Losses ("direct financial loss") resulting directly from the costs to investigate the ransomware attack and prevent further effects of the attack, costs to replace the hardware, costs of reproducing damaged or destroyed data, and the manual processing of orders are not "Direct Financial Loss resulting directly from..." the insured event (and therefore not covered under the Policy) because they required the intervening step of Inchcape deciding to undertake those steps and costs that broke the direct causal chain.

Key Findings
The following factual findings were relevant to the decision:

1. "loss resulting directly from" as used in IA 2 and IA 3 means loss the proximate cause of which is an insured event. However, it is not any "loss" which is covered. It is only "Direct Financial Loss".

2. Exclusion clauses of any indirect or consequential loss will be applied.

Key Takeaways
The decision in Inchcape Australia Limited v Chubb Insurance Australia Limited [2022] FCA 883 affirmed that there will not be direct financial losses resulting directly from the insured events when there is an intervening step(s) by the insured or if those intervening steps would have not necessarily incurred by every insured in the same circumstances.

In addition, the Court's decision means careful attention needs to be given to each cost incurred to see whether it meets the precise causation requirement in the Policy.

Lastly, a cross-reference between Insurance Agreements within a Policy does not necessary mean that the requirements of one insuring clause must be met before another insuring clause can be triggered. The interpretation must be given to the natural and ordinary meaning of the texts in order to figure out the relation between each IAs.

10
References

References

References for smart building cyber security guide

Accenture (2020). Ninth Annual Cost of Cybercrime Study. Retrieved from The Cost of a Cyber Breach (cmswire.com)

Australian Centre for Cyber Security (2022). ACSC Annual Cyber Threat report 2021-22. Retrieved from ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

Australian Centre for Cyber Security (2021). ACSC Annual Cyber Threat Report, July 2020 to June 2021. Retrieved from ACSC Annual Cyber Threat Report, July 2020 to June 2021 | Cyber.gov.au

Australian Competition and Consumer Commission (2022). Scams robbed Australians of more than $2 billion last year. Retrieved from Scams robbed Australians of more than $2 billion last year | ACCC

Cyber and Infrastructure Security Centre (2022). Reporting and compliance. Retrieved from Overview (cisc.gov.au)

Dark Reading (2021). Lights Out: Cyberattacks Shut Down Building Automation Systems by Kelly Jackson Higgins. Retrieved from Lights Out: Cyberattacks Shut Down Building Automation Systems (darkreading.com)

Forbes (2016). Hackers Use DDoS Attack To Cut Heat To Apartments by Lee Mathews. Retrieved from Hackers Use DDoS Attack To Cut Heat To Apartments (forbes.com)

Forbes (2017). Hackers lock down hotel rooms in a new twist on ransom attacks, by Lee Mathews. Retrieved from Hackers Lock Down Hotel Rooms In A New Twist On Ransom Attacks (forbes.com)

Insurance Council of Australia (2022). Cyber Insurance: Protecting our way of life, in a digital world. Retrieved from https://insurancecouncil.com.au/wp-content/uploads/2022/03/Cyber-Insurance_March2022-final.pdf

Joint Cyber Security Advisory (2021). 2021 Trends Show Increased Globalized Threat of Ransomware. Retrieved from 2021 Trends Show Increased Globalized Threat of Ransomware | Cyber.gov.au

NHS England (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack. Retrieved from lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (england.nhs.uk)

Smart Company (2022). Government pushes for tighter cyber security after Optus hack by Tegan Jones. Retrieved from Government pushes for tighter cyber security after Optus hack (smartcompany.com.au)

The Guardian (2021). Personal Details of 80,000 South Australian Public Servants stolen in Cyber-attack, by Royce Turmelov. Retrieved from Personal details of 80,000 South Australian public servants stolen in cyber-attack | South Australia | The Guardian

United States Government Department of Energy (2020) Challenges and Opportunities to Secure Buildings from Cyber Threats. Retrieved from Challenges and Opportunities to Secure Buildings from Cyber Threats | Department of Energy

11
Glossary

Glossary

Glossary of Cyber Security and Smart Building Terms

BAS [Building Automation System]
This network is developed to connect and automate the selected functions throughout the building. This can include but is not limited to lighting, security and fire systems, HVAC systems and more.

BMS [Building Management System]
A 'BMS' can also be known as a building automation system/ energy management system. This system is a computer-based intelligent system which controls and monitors the building's technical systems. This is different from a BAS as this system controls and monitors, whereas the BAS only automates the programs.
Bug Bounty Program: This program offers compensation and recognition to individuals who locate and report vulnerabilities/ bugs or exploits to the organisation running the program.
BYOD: Bring your own device simply means when a member of staff uses their personal technology like laptops, iPads or mobile phones to conduct work related activities.

Essential 8 (ASDE8)
The Australian Signals Directorate (ASD) identified and prioritized 27 strategies for mitigating cyber security incidents. However, the ASD categorized 8 out of these 27 as absolute must haves for any modern organisation and is your bare minimum baseline for your cyber protection framework. While not strictly a cyber security framework, these mitigation strategies help organszations minimise risks and protect themselves from targeted cyber intrusions, Ransomware/external adversaries and malicious internal threats looking to either steal or destroy data.

Exploit
"To use something to one's own advantage." An exploit can use data, software or a sequence of commands to infiltrate systems. Exploits use bugs or vulnerabilities to gain access and control to computers or larger systems. An exploit also gives the attacker an opportunity to increase their system privileges to do real damage.

HVAC
This automated and intelligent system relates only to the Heating, Ventilation and Air Conditioning system of a building. The goal of a HVAC system is to ensure high air quality and optimal air temperature control to the whole building.

IoT
The 'Internet of Things' refers to the countless physical devices globally which are connected to the internet which are all collecting and sharing data. This can range from Boeing 787's all the way down to microchips.

ISO27001
This is a certification which requires businesses to be cyber security compliant to a certain degree. This is a globally recognized framework, which is regarded as a high standard for cyber security compliance. It includes all legal, physical and technical controls which are involved within an organisation's information risk management systems and processes.

MFA/2FA
MFA or Multi Factor Authentication also known as 'two factor authorisation' (2FA) strengthens your security online. After you input your regular password, the MFA platform you're linked to will send you a notification. This will be sent to your chosen back-up e-mail or phone number to confirm it's really you. Imagine this: You're out enjoying a stroll, or a lovely meal and you've received a notification that someone or something is attempting to log into your e-mail account, social media or work networks. Your MFA platform pops up and you select that it is not you attempting to access the account. You then can appropriately mitigate the risk by reporting it to your workplace or changing your passwords on social media accounts. You may have just avoided having your identity or data stolen.

Malicious Actors/Adversary
When these two terms are mentioned, they are referring to a person or group of people who take steps to inflict harm to an organisation or individual through cybercrime. They are commonly referred to as 'hackers'.

Malware
Malware is specifically designed to gain unauthorized access to a device. It's designed to cause damage and disorder. It can sometimes be undetected.

Network Segregation
Network segregation is like organising a group of people into different rooms in a house. Just like you wouldn't want a bunch of noisy kids running around in the same room as a sleeping baby, you wouldn't want all the computers in a network to be able to access each other's information. By dividing a network into different subnetworks, or rooms, we can make sure that only certain computers can talk to each other, which makes the network more secure and efficient.

NIST
Developed by the National Institute of Standards and Technology in the United States, this Cyber Security Framework is a set of guidelines for mitigating risks. Its core functions are to identify, protect, detect, respond and recover. This framework has been recognised globally and is being adopted by large-scale businesses across the world.

Penetration Testing
Penetration testing or Pentesting for short is a process in which an organization's cyber security is put to the test by ethical hackers. While organizations may put cyber security strategies in place, it's hard to know if every hole has been patched and every attack vector considered. This is where an ethical hacker comes in. Ethical hackers (Pentesters) are security experts who are trained to employ the same tricks and techniques as a well-trained adversary. During a Pentest they follow strict methodologies made up of checklists and guidelines ensuring they look for all the common holes that a normal scanner just couldn't pick up in a way that won't damage the infrastructure they are testing.

Phishing
Have you ever received an email or text message from someone that seemed too good to be true? Maybe it was about a free trial, fake parcel or your 'boss' and after checking out the linked website you know something doesn't look quite right. That is called phishing. These malicious groups try anything possible to access your data by luring you in with fake sites, hoping you'll not be educated enough and input your data like credit card information.

Ransomware
Similar to malware, ransomware is a software/program which denies the user of a device by (usually) encrypting their files until a sum of money is paid to gain the decryption code.

Social Engineering:
This term is used to describe a diverse range of malicious activities where the malicious actor uses manipulation tactics to trick their victim into divulging sensitive/ security information. This can occur in isolated events or in multiple attempts.
Trojan: A type of malware that is downloaded onto a device under the guise of a legitimate program/ code or software. It conceals its true content, hence the name.

VPN
The acronym 'VPN' stands for 'Virtual Private Network' and provides a protected network connection when using a public network. VPN's create an encrypted environment online which disguises your identity. The purpose of a VPN is to protect your network from third parties.

Vulnerability
A vulnerability is a flaw or flaws in your systems. These vulnerabilities are exploited by malware and/or an attacker. Dysfunctional systems can lead to hackers getting inside your network, which could result in them stealing data, giving themselves access to certain systems and launching attacks on a device or devices. How can I make my systems less vulnerable? Firstly, if you're not a cyber security professional it can be very difficult to spot holes in your systems. We recommend leaving it to the professionals and letting them patch holes and reconfigure systems for optimal protection of your data. Human error is the largest threat to the cyber security architecture. Errors made by humans can expose data or create exploitable access points for hackers. Such as opening a phishing e-mail or not keeping software up to date. Network vulnerabilities like unsecure Wi-Fi, old hardware and out of date software are high contributors to vulnerabilities in your systems.

WiredScore
WiredScore is the global digital connectivity certification that evaluates, improves, benchmarks and promotes best-in-class connectivity in the built world. (Taken from WiredScore website).

13
Authors

Authors

Charlie Hales
Managing Director, Waterstons Australia

Ric Navarro
Head of Clients and Marketing, Cundall

Ryan O'Kell
Head of Cyber Security, Waterstons Australia

Claudia Oprya
Marketing Manager, Waterstons Australia

Annie Nguyen
Principal, Building Automation, Cundall

Hartmut Kraft
Principal, Security, Cundall

Qucheng Yan
Senior Engineer, Cundall

Pouyan Aski
Senior Electrical Engineer, Cundall

Willow Aliento
Corporate Journalist, Cundall

Contact us

Waterstons

Charlie Hales - Managing Director
Charlie.hales@waterstons.com
T 0427 432 873

Claudia Oprya - Marketing Manager ANZ
Claudia.oprya@waterstons.com
T 0404 723 752

Waterstons Pty
4.03 6 Eden Park Drive
Macquarie Park, Sydney
NSW, 2113

Office +61 2 9160 8430
Service desk +61 2 9160 8445
Email info@waterstons.com.au
Get In Touch | Waterstons Australia

Cundall

Julian Bott - Managing Director, APAC
j.bott@cundall.com
T +61 (0)2 8424 7000

Singapore
111 Somerset Road
Unit #07-20 111 Somerset, 238164
Singapore
T +65 6911 2600
singapore@cundall.com

Hong Kong
7/F and 8/F, The Hennessy
256 Hennessy Road
Wanchai, Hong Kong
T +852 2688 2318
hongkong@cundall.com

Adelaide
Kaurna Country
Level 1, 89 Pirie Street
Adelaide, SA 5000, Australia
T +61 (0)8 8419 2700
adelaide@cundall.com

Brisbane
Turrbal Country
Level 6, 25 King Street, Bowen Hills
Brisbane, QLD, 4006, Australia
T +61 (0)7 3607 5700
brisbane@cundall.com

Melbourne
Wurundjeri Woi Wurrung Country
Level 14, 500 Collins Street
Melbourne, Vic, 3000, Australia
T +61 (0)3 9635 3700
melbourne@cundall.com

Perth
Whadjuk Noongar Country
Level 2, 585 Hay Street
Perth, WA, 6000, Australia
T+61 (0)8 9421 3700
perth@cundall.com

Sydney
Cammeraygal Country
Level 6, 99 Mount Street
North Sydney, NSW, 2060, Australia
T +61 (0)2 8424 7000
sydney@cundall.com

Waterstons

www.waterstons.com.au

CUNDALL

www.cundall.com