Centre for
**Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey & Company

# 2021 Cambridge - McKinsey Risk Prize

# Bio-sketch and Photo Page

**Student Name:** Sheryn GILLIN

**Email contact:** sg887@cam.ac.uk

**Title of Submission:** Cybersecurity Risk to Healthcare from Building Services

**I am a candidate for the degree:**

MSt in Construction Engineering

**Bio-sketch**

Sheryn is undertaking a MSt (part-time) in Construction Engineering, run by the Department of Engineering, in association with the Judge Business School.

Sheryn has over 30 years' experience as an electrical, controls and project engineering professional in Australia, Canada, New Zealand and the USA. She has gained knowledge of the construction industry, mining, oil & gas, water, electricity generation, pulp & paper, defence and government sectors through the delivery of medium to large scale multi-discipline engineering projects.

For the past 5 years Sheryn has been involved in the integration and commissioning of systems at a superhospital in Montreal Canada and 3 hospitals in the UK. Experiencing first-hand the cybersecurity risk to healthcare from building services was her driver for this research.

Centre for
**Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

McKinsey & Company

# *CYBERSECURITY RISK TO HEALTHCARE FROM BUILDING SERVICES*

**Sheryn GILLIN**

**April 2021**

Centre for
**Risk Studies**

UNIVERSITY OF
CAMBRIDGE
Judge Business School

McKinsey
& Company

# 2021 Cambridge - McKinsey Risk Prize

# Declaration Form

**Student Name:** Sheryn GILLIN

**Email contact:** sg887@cam.ac.uk

**Title of Submission:** Cybersecurity Risk to Healthcare from Building Services

**Number of words of submission:** 2598 (with references 3347)

**I am a candidate for the degree:** MSt in Construction Engineering

**Academic Institution/Department:** Dept. of Engineering

**Declaration**

I confirm that this piece of work is my own and does not violate the University of Cambridge Judge Business School's guidelines on Plagiarism.

I agree that my submission will be available as an internal document for members of both Cambridge Judge Business School and McKinsey & Co's Global Risk Practice.

If my submission either wins or receives an honourable mention for the Risk Prize, then I agree that (a) I will provide a recorded 2 minute overview of my paper, (b) my submission can be made public on a Cambridge Judge Business School and/or McKinsey & Co websites.

This submission on risk management does not exceed 10 pages.

Signed Gill

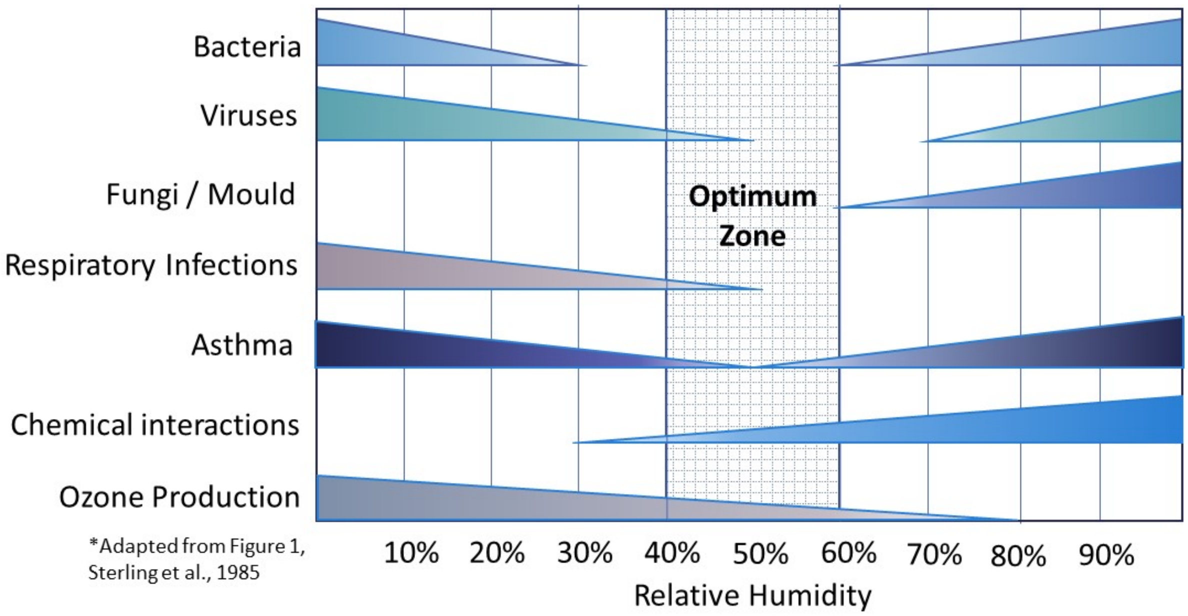
Please include this declaration form after the cover page of your paper submission.

# 1 INTRODUCTION

The theft of electronic health records and the vulnerability of medical devices are perceived as the foremost cybersecurity risks in the critical infrastructure sector of healthcare; this limited view, however, overlooks the building services that maintain the environment within rooms central to the treatment of patients, such as operating theatres, laboratories, pharmacies, sterile stores and diagnostic imaging rooms [1, 2]. To achieve the optimal humidity in these specialist areas, the chilled water system must function within set tolerances. Any divergence places patients at risk due to Healthcare Associated Infections (HAI) or cancelled surgeries / diagnostic procedures.

## 1.1 The importance of humidity control

In 1985 Sterling et al. [3] reviewed over 70 scientific articles, related to the effect of humidity on biological contaminants such as bacteria, viruses, and mould, airborne pathogens causing respiratory infections, and the speed of chemical interactions including ozone production. The graphical representation of this research - known as the Sterling Diagram (reference Figure 1) - is still referenced in industry today. Bar width indicates effect or population; relative humidity (RH) is the amount of water vapor in air as a percentage of how much moisture the air could hold at the same temperature. To minimise the risk to human health, clinical spaces must remain within the optimal zone of 40 - 60%RH [3].



*Adapted from Figure 1, Sterling et al., 1985

**Figure 1 - The Sterling Diagram**

Patients and staff are at risk when the RH is <40% because bacteria and viruses travel long distances on droplets and skin flakes [4, 5], whilst medical equipment failures increase due to Electrostatic Discharge (ESD) [5, 6]. When the RH is >60%, microorganisms wick through packaging materials affecting sterility and shelf life [7, 8], condensation forms on electronic circuits [9] causing failures, and patients are directly at risk because moisture decreases the efficiency of drugs [10, 11].

### 1.2 The importance of the chilled water system

Dehumidifying the air to maintain the temperature and RH within the optimal zone requires chilled water; this system is also vital to the efficient operation of Magnetic Resonance Imaging (MRI) machines and Computerised Tomography (CT) scanners.

The wire coils used to generate the magnetic field in an MRI are cooled using liquid helium, which vaporises in the process. Chilled water is then used to recondense the gas/vapor before the liquid helium is recirculated [12]. If the gaseous helium cannot be cooled it must be safely vented to atmosphere in what is called a quench. To prevent a quench, imaging operations must be postponed until adequate cooling is available; without this mitigation measure, an MRI will remain out of service for several days until the liquid helium can be replaced.

Whilst not essential for a CT scanner to function, chilled water can increase patient throughput by reducing the time required to cool the x-ray tubes. Given tubes can take up to 30 minutes to cool without assistance [12] the use of chilled water to transfer heat from the tubes could double throughput, providing hospitals with an improved return on their investment.

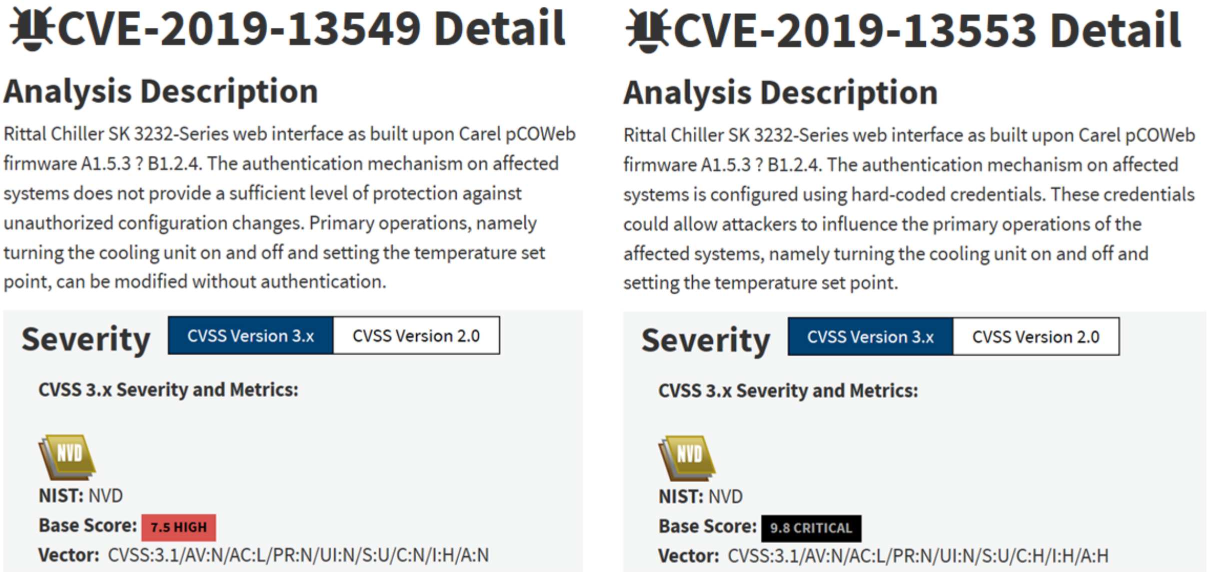
In summary, a cyber-attack on a hospital's chilled water system, could place patients and staff at risk due to HAIs, the cancellation of imaging procedures, forfeiture of revenue, or damage to high-value medical equipment.

## 2 Cyber-attack Scenario

The following example illustrates an actual chiller vulnerability and describes the impact to hospital operations should this, or a similar weakness, be exploited.

### 2.1 Vulnerability

Major chiller manufacturers, such as Carrier and Rittal, employ the same controller: a Carel pCOWeb. Figure 2 is an extract of two Common Vulnerabilities and Exposures (CVEs) records from the (US) National Vulnerability Database, dated July 2019; the entries describe how hackers can turn off cooling and/or modify a chillers' temperature setpoint. The typical remedial action of patching the vulnerability is not an option in this case as no firmware update will be published because the controller has been obsolete since December 2017 [13, 14].



CVE-2019-13549 Detail

Analysis Description

Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems does not provide a sufficient level of protection against unauthorized configuration changes. Primary operations, namely turning the cooling unit on and off and setting the temperature set point, can be modified without authentication.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 7.5 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVE-2019-13553 Detail

Analysis Description

Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems is configured using hard-coded credentials. These credentials could allow attackers to influence the primary operations of the affected systems, namely turning the cooling unit on and off and setting the temperature set point.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 9.8 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Figure 2 - Chiller Controller Vulnerability**

## 2.2 Modifying the Temperature Setpoint

### 2.2.1 High Relative Humidity

Modifying the temperature setpoint of a chiller could result in a facility being unable to dehumidify the intake air to maintain 40-60%RH. The impact and duration will be dependent on the properties of the outside air, as even under ideal starting conditions, temperature and humidity in a facility will increase due to exhalation [15] and the heat generated by hospital and laboratory equipment [16]. High RH in sterile storage areas may necessitate the destruction of product, whilst in operating theatres, all but emergency surgeries will be rescheduled due to the unsuitable working conditions for staff and risk of infection to patients. The direct cost of destroying materials can be easily calculated. Healthcare Associated Infections though, are more difficult to quantify as a percentage of the annual HAIs. In 2009, a submission to the Australian Government Productivity Commission noted 150,000 HAIs per year, contributing to 7,000 deaths at a cost of AUD$954million [17], whilst in the UK in 2007, the figures were 300,000 infections, 9,000 deaths, costing £1billion [18].

### 2.2.2 Decreased Heat Transfer

Increasing a chillers' temperature setpoint decreases the ability of the chilled water system to absorb heat [19]. When less heat is removed the magnet of an operating MRI cannot be cooled. In this scenario, there are two options: halting imaging services, which could cost a nonsocialised healthcare facility over $US40,000 per day in revenue [20] or continuing and risk a quench, which could cost upwards of £20,000 to refill the MRI with liquid helium [21].

## 2.3 Turning off the cooling unit

Chillers are classified as critical, and therefore installed as N+1, meaning the loss of one chiller will not impact the ability to provide environmental control to specialist areas or cool high-value imaging equipment. To prioritise the delivery of chilled water to critical areas though relies on human intervention to increase the supply air temperature of ventilation systems serving non-critical areas.

# 3 Risk Mitigation

No other critical infrastructure sector has such reliance on both Information Technology (IT) and Operational Technology (OT). Some sectors, like finance, are heavily reliant on IT; others, such as water, energy, or manufacturing, primarily rely on OT. Therefore, it is difficult to draw comparisons between healthcare and other sectors. However, what is acknowledged, is the below average IT and cybersecurity budgets within healthcare [22,23]. With two attack fronts: IT for electronic health records and medical devices, and OT for building services, these budgetary constraints are concerning given the recent increase in cyber-attacks on healthcare providers [24].

This section focusses on four areas where the parties involved in delivering healthcare projects can make small changes to ensure cybersecurity is at the forefront of decision making throughout the design and construction stages. If these changes are not made, healthcare providers will continue to spend their limited budget remedying the resilience of design, modifying the network architecture, or updating the equipment procured [25, 26] to minimise the facilities cybersecurity risk. These savings could instead be put towards hiring a specialist with OT cybersecurity skills.

Four case studies were used in this research: Centre Hospitalier de l'Université de Montréal (CHUM), Royal Liverpool University Hospital (RLUH), Brighton Sussex University Hospital (BSUH) and Specialist and Critical Care Centre (SCCC).

## 3.1 Contract & Procurement

CHUM and RLUH were Public Private Partnership (PPP) / Private Finance Initiative (PFI) contracts. Under this type of contract, it could be argued that unless specifically listed as a Relief Event or Force Majeure, the disruption and unavailability of areas in a hospital due to a cyber-attack, is the responsibility of the Consortium, especially in the current environment.

Clauses must be included in PPP/PFI contracts to ensure both parties are aware of their obligations and responsibilities from design through to updates / maintenance as well as who is accountable for fault diagnosis and remedial measures, should a cyber-attack occur.

BSUH and SCCC were different versions of the New Engineering Contract (NEC) adopted by governments worldwide. Under NEC, the frustration / force majeure clause (19.1) is in respect to the construction, not the design or delivered asset. The term 'cyber' did not exist in the case study contracts or works information. The optional Standard Boilerplate Amendments to the current version, NEC4, dated January 2019, introduced clause Z101 titled Cyber Essentials [27]. This section however only refers to a Schedule requiring the Contractor provide a Cyber Essentials Certificate prior to the works commencing. An important step, but this UK Government Scheme operated by the National Cyber Security Centre (NCSC) must move from being aimed at the construction company, to the project deliverable. Cybersecurity assurance must also be passed down to each subcontractor who provides equipment with software, firmware or an ethernet/USB port.

If cybersecurity is not included in the contract, there are some low-cost improvements the construction industry can consider as part of the procurement process. A review of the Procurement Templates from each case study highlighted that there are no standard clauses or requirements related to cybersecurity when procuring building service equipment with control functionality. Standardised clauses should be added to all procurement templates to ensure suppliers understand they have an obligation to fully disclose the firmware, software and communication ports procured as part of a system; this includes any open source software.

## 3.2 Design

### 3.2.1 Design Life

The mechanical equipment installed in a facility are typically designed to last for decades [26]. Electronic components though do not have the same design life, as was highlighted with the obsolescence of the pCOWeb controller cards. Imagine being the operator of a new healthcare facility handed over in 2016, possibly finding out in 2019 that your chiller has a known vulnerability that will never be patched. Without specific clauses in the contract the owner/operator will be facing unplanned remedial works, from an already stressed budget. That is, provided the owner is aware of the software and firmware details and has been undertaking regular vulnerability checks. To minimise risk, manufacturers of controllable devices must be encouraged to ensure there is an upgrade path and ongoing support for the whole life of the equipment [28].

### 3.2.2 Secure by Design

In the construction industry, redundancy and resilience tends to have a narrow interpretation, based around the loss of power or a hardware failure. Building services engineers must now expand that ‘what if’ thinking to include possible cyber-attacks and this analysis must be done from project conception to minimise the cybersecurity risk [25]. Questions regarding network architecture, Virtual Local Area Networks (VLANs) versus a single broadcast domain [29], even ‘old technology’ such as volt-free contacts should form part of the analysis. These details must be decided early in the project lifecycle, with input from the team who will operate and maintain the asset, to minimise the risk from a cyber-attack.

As there are no laws mandating cybersecurity certification in the healthcare sector [30], clients should not expect Design Consultants to automatically include a cyber-secure design post contract signing. The Standard Specifications, including those related to the OT systems, from the 4 different Service Consultants working on the case study hospitals, did not go to that level of detail, nor did the case study contracts referenced the ISA/IEC 62443 framework [31], designed to address the security of ICS. Perhaps these standards are not included because Building Service Integrators do not view their discipline as Industrial Control, but given the protocols have the same inherent flaws, the construction industry must begin to apply these standards. ISA/IEC 62443-3-3 for example, provides 51 system requirements to improve the resilience to cyber-intrusion in OT systems. This would be the ideal starting point in the design of Building Services for Critical Infrastructure Projects.

### 3.2.3 Software Quality Assurance

All software delivered on critical infrastructure projects must be as robust as possible. On each of the case study hospitals neither the Constructor nor Subcontractors had a Software Development policy; the only company standards were in relation to internal IT applications. In other critical infrastructure industries such as defence, code reviews on in-house software is standard. The procedure is used to verify that all requirements have been addressed and the logic sound before any software is deployed. This avoids applying quick patches during commissioning to resolve a failed test, without fully understanding the implications to other programs. Not applying this rigor to any software delivered as part of a project can leave hospitals vulnerable.

Periodically reviewing the software is also important given the concerns over sleeper software intended to sabotage critical infrastructure [32]. However, not all Facility Management (FM) Teams have the skill set required to review code [33]. With the skills shortage, especially in OT, perhaps this process can be automated, and executed quarterly.

Clotet et al. [34] noted companies are reducing costs by adopting standard embedded Commercial-Off-The-Shelf (COTS) products, like the chiller manufacturers did with Carel pCOWeb. These third-party details must also be part of the software quality assurance procedure, and ensure manufacturers set aside funding to maintain the software and compilers [28] for the full life of the product.

None of the Operations & Maintenance (O&M) Manuals produced for the case study projects listed the firmware version of any Original Equipment Manufacturer (OEM) controllers. Not surprisingly, given these manuals are typically generated electronically from the manufacturer's literature provided during the procurement process. Even if the Constructor asks for the firmware and software details, the subcontractor tasked with collating the documentation must ensure a field is available in the template to populate. Patching of an IT switch stack will not be shown in a BIM model; this data will only reside in the O&M Manual or software management application.

# 4 Conclusion

Three years have passed since WannaCry crippled the NHS, and with the first death attributed to a cyber-attack in 2020 [35], it is time for the construction industry to begin evaluating the cybersecurity risks of critical infrastructure projects at the earliest stages of design and procurement.

A cyber-attack targeting a chiller can severely disrupt a healthcare facility and endanger patient's health because chilled water is indispensable for an MRI to operate and is also required to maintain the environment necessary to minimise infections and safely store sterile products. To minimise this risk, several recommendations, regarding construction contracts, procurement, design and documentation were proposed.

Taking cybersecurity into consideration in contracts, design and procurement will be novel to many in the industry. Government and clients must participate in this change by ensuring the contract requirements clearly establish the cybersecurity requirements. Building services engineers are adept at considering risk, redundancy and resilience, from a siloed discipline perspective; this process must now be applied, with cybersecurity in mind. Expertise in the field is not mandatory, but everyone does need to question whether a device has a controller (software, firmware, communications port), and if so, what measures should be employed to minimise the cybersecurity risk. Those procuring equipment must also play their part, by asking whether a mechanical device has an electronic controller. If so: ensure the software and firmware version is provided, search the vulnerability database, and ask the subcontractor for their cyber assurance certification.

The risk review was only performed on the chilled water system installed in the four case study hospitals. No evaluation was undertaken to determine if this is the most critical building service. Therefore, many systems, which could disrupt a hospital, remain to be evaluated and categorised. This step is vital to ensure a cybersecurity risk management strategy focusses on and protects the most critical assets.

These recommendations are crucial to minimising the risk to healthcare from building services by providing an awareness of the issue and encouraging change to ensure the limited IT and cybersecurity budget is not spent addressing the deficiencies of newly constructed assets.

# 5 References

| | |
|---|---|
| [1] | AAMI (Association for the Advancement of Medical Instrumentation). (2015) *Relative Humidity Levels In The Operating Room. Joint Communication to Healthcare Delivery Organizations*. Available at: https://www.aami.org/docs/default-source/uploadedfiles/filedownloads/news/humidity-in-or-joint-communication-to-hdos-january-2015.pdf (Accessed: 15 May 2020). |
| [2] | Medicines and Healthcare Products Regulatory Agency (MHRA). (2015) *Safety Guidelines for Magnetic Resonance Imaging Equipment in Clinical Use.* London, MHRA. |
| [3] | Sterling, E.M., Arundel, A. and Sterling, T.D. (1985) 'Criteria for human exposure to humidity in occupied buildings'. *ASHRAE Transactions*, 91(1), pp. 611-622. |
| [4] | Binder, L. (2019) *This Inexpensive Action Lowers Hospital Infections And Protects Against Flu Season*. Available at: https://www.forbes.com/sites/leahbinder/2019/10/17/harvard-researcher-says-this-inexpensive-action-will-lower-hospital-infection-rates-and-protect-us-for-the-flu-season/?sh=6651db418247 (Accessed 30 July 2020). |
| [5] | Bennett, D. (2019) *Health and Humidity: Fundamentals / Applications / Research*. |
| [6] | Kohani, M. and Pecht, M. (2016) 'New Minimum Relative Humidity Requirements Are Expected to Lead to More Medical Device Failures'. *Journal of Medical Systems*, 40(3), pp. 1–6. |
| [7] | Infection Control Today. (2018) *Maintaining Proper Sterile Storage Conditions*. Available at: https://www.infectioncontroltoday.com/view/maintaining-proper-sterile-storage-conditions (Accessed 24 July 2020). |
| [8] | U.S. Food and Drug Administration. (2020) *Medical Devices That Have Been Exposed To Heat And Humidity.* Available at: https://www.fda.gov/medical-devices/emergency-situations-medical-devices/medical-devices-have-been-exposed-heat-and-humidity (Accessed 5 April 2020). |

[9] Schoppe, G. (2019) The Facts In MRI Artifacts. Available at: https://www.keimedicalimaging.com/post/the-facts-in-mri-artifacts#! (Accessed 11 July 2020).

[10] Medecins Sans Frontieres (n.d.) *Drug quality and storage.* Available at: https://medicalguidelines.msf.org/viewport/EssDr/english/drug-quality-and-storage-16688167.html (Accessed 24th July 2020)

[11] Polygon (n.d.) Monitoring Humidity in Pharmaceutical Storage. *Temporary Climate Solutions.* Weblog. Available at: https://www.polygongroup.com/en-US/blog/monitoring-humidity-in-pharmaceutical-storage/ (Accessed 24th July 2020).

[12] Brown, J. and Turra, F. (2020) Water Chilling for Temperature Control in MRI and CT Scanners. [Blog] Available at: <http://blog.parker.com/water-chilling-for-temperature-control-in-mri-and-ct-scanners> [Accessed 14 March 2021].

[13] Redteam-pentesting.de. (2019) Available at: https://www.redteam-pentesting.de/de/advisories/rt-sa-2019-013.txt (Accessed 27 July 2020).

[14] Redteam-pentesting.de. (2019) Available at: https://www.redteam-pentesting.de/de/advisories/rt-sa-2019-014.txt (Accessed 27 July 2020).

[15] Mansour, E., Vishinkin R., Rihet S., Saliba W., Fish F., Sarfati P., and Haick H. (2020) 'Measurement of temperature and relative humidity in exhaled breath', *Sensors and Actuators B: Chemical*, p. 304.

[16] ASHRAE (American Society of Heating, Refrigeration and Air Conditioning Engineers). (2001) *ASHRAE Fundamentals Handbook (SI) - Nonresidential Cooling and Heating Load Calculation Procedures*. Atlanta, ASHRAE. P.29.9.

[17] Becton Dickinson. (2009) *Healthcare Associated Infections*. Submission to the Commission on Performance of Public and Private Hospital Systems. Available at: <https://www.pc.gov.au/inquiries/completed/hospitals/submissions/sub029.pdf> (Accessed 2 April 2021).

[18] National Institute for Health and Care Excellence. (2012) Healthcare-associated infections: prevention and control in primary and community care. Clinical guideline [CG139]. Available at: <https://www.nice.org.uk/guidance/cg139/chapter/introduction> [Accessed 2 April 2021].

[19] Taylor, S.T. (1995) Degrading Chilled Water Plant Delta-T : Causes and Mitigation.

[20] Thoma, C. (2018) Why MRI Machine Cooling is Critical to Reliability and Patient Satisfaction. [Blog] *Welcome to the Schneider Electric Blog – Healthcare*, Available at: https://blog.se.com/healthcare/2018/03/23/mri-machine-cooling-reliability-patient-satisfaction/ (Accessed 13 April 2020).

[21] Kramer, D. (2019) 'Helium users are at the mercy of suppliers', *Physics Today* 72, 4, 26. Available at: doi: 10.1063/PT.3.4181

| | |
|---|---|
| [22] | Weins, K. (2020) IT Spending by Industry. [Blog] Available at: <https://www.flexera.com/blog/industry-trends/it-spending-by-industry/> [Accessed 17 March 2021]. |
| [23] | Morgan, S. (2019) *The 2020 Healthcare Cybersecurity Report*. Available at: <https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf> [Accessed 17 March 2021]. |
| [24] | Alder, S. (2021) Healthcare Industry Cyberattacks Increase by 45%. *HIPAA*, Available at: <https://www.hipaajournal.com/healthcare-industry-cyberattacks-increase-by-45/> [Accessed 2 April 2021]. |
| [25] | Coventry, L. and Branley, D. (2018) 'Cybersecurity in healthcare: a narrative review of trends, threats and ways forward'. *Maturitas*, 113, pp. 48-52. |
| [26] | Felser, M., Rentschler, M. and Kleineberg, O. (2019) 'Coexistence Standardization of Operation Technology and Information Technology'. *Proceedings of the IEEE*, 107(6), pp. 962-976. |
| [27] | NEC, (2019) NEC4-Engineering and Construction Contract Z: boilerplate clauses. Crown Commercial Services. |
| [28] | Anderson, R. (2018) 'Making security sustainable'. *Communications of the ACM*, 61(3), pp. 24-26. |
| [29] | Zimba, A., Wang, Z., and Chen, H. (2018) 'Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems'. *ICT Express*, 4(1), pp. 14-18. |
| [30] | Abraham, C., Chatterjee, D. and Sims, R.R. (2019) 'Muddling through cybersecurity: Insights from the U.S. healthcare industry'. *Business Horizons*, 62(4), pp. 539–548. |
| [31] | IEC/PAS (International Electrotechnical Commission / Publicly Available Specification). (2008) IEC/PAS 62443-3:2008. *Security for industrial process measurement and control – Network and system security.* International Electrotechnical Commission. |
| [32] | Benson, S. (2021) Spy threat to overtake terrorism. *The Weekend Australian*, pp.1-2. |
| [33] | Gillin, S. (2019) 'Facility Management barriers to the operation of sustainable building services: a UK Constructor's Perspective' CEM08. University of Cambridge. Unpublished essay. |
| [34] | Clotet, X., Moyano, J., and León, G. (2018) 'A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of Critical Infrastructures'. *International Journal of Critical Infrastructure Protection*, 23, 11-20. |
| [35] | Williams, R. (2020) *Woman Dies After German Hospital Is Targeted By Cyber Attack*. Available at: https://inews.co.uk/news/technology/germany-hospital-cyber-attack-woman-dies-ransomware-duesseldorf-652997 (Accessed 18 September 2020) |