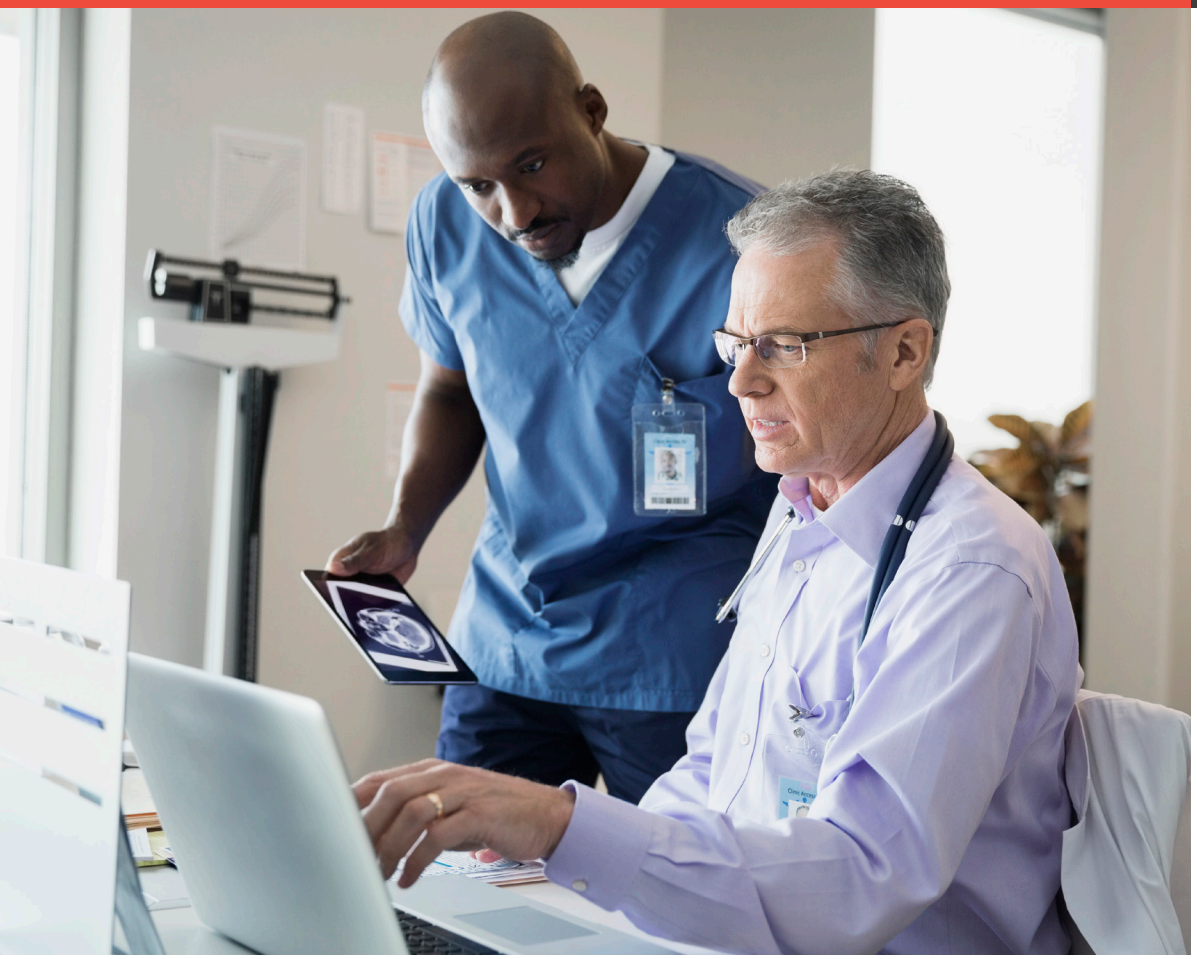
The unseen danger: cyber security threats to hospitals' operational systems

How to protect life-critical Operational Technology (OT) systems in healthcare



pwc

Facing up to the unknown risk in hospitals

Picture the scene. You're the general manager of a large urban hospital with more than 1,000 beds. Every one of those beds has an oxygen supply point installed next to it. One morning, you get an alert that the flow of oxygen to each of the beds has been cut off.

This is putting patients' lives in danger. In desperation, medical staff are trying to move patients and their beds to other floors where they think oxygen may still be available. But they find that the elevators have stopped working, leading to a logjam in the corridors.

Then you get another message. The air conditioning system throughout the building has failed. This is causing the temperature to rise rapidly in the intensive care wards and operating theatres – further endangering lives and forcing in-flight medical procedures to be suspended.

The result? The hospital is effectively paralyzed. It's then that you receive your first communication from the cybercriminals whose attack has caused the chaos. They're about to name their terms for allowing your operations to restart.

…hidden in the OT 'blind spot'

If this sounds like science fiction, it shouldn't. Because many hospitals' operational technology (OT) systems are worryingly vulnerable to this type of cyber breach. And there is a growing range of adversaries – from blackmailers to terrorists to hostile nation states – who might be contemplating mounting such an attack. Also, while the COVID-19 pandemic hasn't increased the vulnerability of hospitals' OT, it has boosted the societal importance of well-functioning health facilities, thus making them potentially more attractive targets. Imagine if a foreign power had a 'red button' that could cut off oxygen to every hospital bed in a country.

Given all this, why isn't healthcare OT better protected against cyberattacks? The reality is that the current focus of health organisations' cybersecurity efforts tends to be on protecting information technology (IT) and medical data rather than OT. It isn't hard to see why. In recent months and years, many hospitals' IT systems have suffered ransomware breaches, often involving criminals stealing or encrypting vital data – including patient information – and then demanding a ransom to release it. A recent example was the fatal attack **on Düsseldorf University Hospital (see information panel on Germany).**

The threat of such attacks features increasingly prominently on hospitals' risk radars. But the danger is that by focusing on protecting their IT assets, they may overlook another risk that is potentially at least equally catastrophic: the threat to 'low-tech' devices that are part of the Building Management Systems (BMS) which are themselves part of the hospital's OT network and which play a vital but largely unrecognized role in preserving and saving lives.

The 'blind spot' around cyber risks to hospitals' OT is often baked into organisational structures. In most hospitals, the Chief Information Security Officer (CISO) – accountable for defending the organization against cyberattacks – is responsible only for the IT assets, not OT. This means nobody is looking out for the risks to OT devices and systems. Even worse, in many private medical centers there is no CISO at all, increasing the risks still further.

Germany: public funding for cyber security[1]

Germany experienced a stark reminder of the cyber threats facing hospitals. This occured in September 2020, when Düsseldorf University Hospital was subject to a ransomware attack on its IT systems. The attack was inadvertent, with the cybercriminals thinking they were attacking the university itself. But the collateral damage was catastrophic: the attack meant the hospital was unable to admit a female patient, who subsequently died – the first known death in consequence of a cyberattack. Even before this tragic incident, Germany was in the forefront of action to address cyber threats to hospitals. The German Government recently introduced legislation allocating €4.3 billion of public funding for digitalization and security in hospitals. Regulations in Germany also impose penalties on hospitals that fail to digitize their activities with proper cyber protection.

[1] Source BBC News from 18 September 2020

OT cyber risks in hospitals mirror other industries

All organisations with a building where people work – not just hospitals, but others ranging from office premises and department stores to manufacturing plants – use an OT network to control the environment and facilities within the physical site.

Unlike IT systems and networks, the OT infrastructure focus is not to store, retrieve and use data. Instead, it is focused on monitoring and operating these vital physical functions. In a hospital, these functions are often specific to healthcare – but the overall OT architecture still mirrors the world of Industrial Control Systems (ICS) in other sectors.

A key element of the OT network in hospitals is the BMS, which is responsible for process control throughout the structure, irrespective of whether it is a 'smart' building. In most modern buildings, the control system is designed to respond to specific occurrences by triggering active processes. So – in the case of a hospital – ongoing measurement and monitoring of the temperature in different areas enables the BMS to keep the air-conditioning and/or heating at the right level for staff and patients. Similarly it controls lighting, ventilation openings and security and safety devices. Elevators are also closely monitored and managed.

Another area actively targeted by threat actors during recent breaches was the integration technology layer separating or transporting data between the IT and the OT infrastructure – raw imaging data from scanners to computer processing – for example. The heightened threat to people's health and safety makes the business continuity aspect of hospitals' hybrid IT/OT operations even more important, meaning it's vital that they have robust alternative methods for maintaining services in the event that the integration layer is compromised.

…but the impact of breaches can be many magnitudes greater

However, while the principles of OT are similar between hospitals and other types of building, the potential impact of a cyberattack that shuts down the OT network are generally far bigger in hospitals. Take a residential building: loss of the OT here will normally result in some discomfort and possibly financial loss. But in a hospital – as vividly illustrated by the scenario we described at the start of this paper – the implications are many magnitudes greater. Rather than being merely inconvenient, failed air-conditioning and stranded lifts create a situation where people who would otherwise have lived will potentially die. That's aside from the impact of – for example – power or water being cut off from vital medical devices.

The accompanying information panel describes how such OT risks can be quantified. And they may arise in some unexpected places. Take the building infrastructure and facilities management systems like lights, door opening mechanisms, elevators or air-conditioning. While these systems have often been in use for decades, they're now mostly controlled by digital applications, and are often connected to the Internet. An adversary who gains control over these systems could effectively shut down the hospital's operations – putting the management under severe pressure to pay whatever ransom was being demanded.

An even more critical system in a hospital is the one that delivers water and gas throughout the building. The fact that the system supplies hot water, compressed air and medical gases – oxygen, nitrogen, and so on – wherever and whenever needed, makes it absolutely pivotal to the hospital's delivery of healthcare to patients. The infrastructure that takes oxygen to every bed is essentially a large ICS, with an oxygen tank at one end controlled by a standard controller, and a monitoring system at the other to supply oxygen to the patients on demand. The potential implications of damage inflicted on the controller of this utility system are clear.

Quantifying cyber risks to hospital OT

The impact levels of the cyber risks to OT systems are calculated in a different way from those to IT systems. While in each case the underlying or 'cold' level of risk is calculated based on the degree of threat that is likely to occur, with OT systems it's common practice to add another multiplier: the consequence or 'meaning' of the attack. The meaning helps us to produce the impact-variable for the attack, which is the potential damage resulting from the materialization of the risk. Taking the disabling of a lift or air conditioning system as an example, the 'cold' risk would be relatively low, but the potential impact of this happening in a hospital would be far greater.

OT system risks: layers and controls

In terms of cyber risks, each of the diverse systems within a hospital's overall OT network shares a common characteristic: they all have a chain of supply and support (commonly referred to as the system's supply-chain), that is completely detached from the organizational cybersecurity loops that have been created to safeguard the hospital's IT assets. The effect is that these supply-chains offer various vectors for attacking the OT systems themselves, through methods ranging from remote control through installation of malicious software by disaffected insiders, to connectivity between systems – both OT-OT and even OT-IT – creating the risk of intruders accessing a 'back door' into critical hospital's IT systems as well.

What's more, it's becoming ever more apparent that OT systems now surround all of us in our daily lives – and the fact that they're increasingly the target of cyberattacks – should serve as a warning to hospitals and medical centers. In April 2020, several water management facilities run by a water authority suffered cyber attacks that were luckily thwarted by the company's cyber division. The OT systems at a hotel in Austria have reportedly been hacked four times in ransomware attacks, locking guests out of their rooms. A security firm reported that in 2018, malicious activity targeting ICS affected more than 47% of the industrial computers it was protecting.

To date, cases of similar attacks on hospitals' OT are – fortunately – still rare. But, even as the COVID-19 pandemic plays out, it's probably just a matter of time before healthcare OT comes into the sights of cyber adversaries. And, as we noted earlier, the challenges for hospitals looking to prepare for such attacks are heightened by the fact that most of their IT teams are focused – in many cases overloaded – on protecting organizational IT and data rather than OT, leaving them at risk. There's also a lack of relevant regulation around cyber security standards for healthcare OT systems.

To help map out a viable response, it's useful to visualize OT risks as a stack of layers. At the top are the assets controlling and monitoring operational activities throughout the hospital. Below that are the threats and threat actors potentially targeting the OT assets. The next layer is the risk of these threats actually coming about. And the 'bottom line' is the impact – which in some industries can be mainly reputational or financial, but for a hospital, it comes down to the threat to human life. The controls to manage all these layers fall into three categories: Processes, such as formal procurement procedures to ensure that all purchases and end-of-life disposals of technical equipment follow a set guidelines and adhere to standards for cyber protection; People, including awareness and training around cyber security; and Technological, such as end-point protection, firewalls and appropriate network architecture. All these three elements – processes, people and technology – adding up to the commonly used acronym 'PPT', must be covered for controls to be effective.

A four-step roadmap to address OT cyber risks

As we prepare for a post COVID-19 world how can hospitals and other healthcare facilities defend their OT assets and devices most effectively against cyber threats? At the core, the issue is that advances in OT – including internet connectivity and capabilities for remote control and monitoring – have outpaced awareness of the new and unforeseen risks that these developments inevitably create. Hospitals need to close this gap.

To do this, many hospitals decide to start by buying 'defense boxes' and protection 'gadgets'. However, before buying anything, it's vital to have a clear view of the OT assets and the actual risks they need to be protected against. With this in mind, here's a practical four-step approach that we've found can enable a hospital to improve its OT cyber resilience:

1

Understand and communicate that the risk exists

The starting-point is to understand and recognize that there are potentially critical risks in OT systems (not just IT) and build awareness and buy-in at the board level that these risks need to be addressed. Without rock-solid commitment at senior management levels, the necessary investment in OT cyber security won't happen. With senior buy-in established, the Organisation's management can assess the key vulnerabilities of its OT assets, and outline a path for managing the resulting risks without compromising the hospital or medical center's operational continuity.

2

Chart the OT assets and organizational maturity

With the case for action clearly established, management should carry out a preliminary survey to chart the OT assets and related risks. In parallel, it's important to gain an in-depth familiarity with the maturity level of the organization regarding cybersecurity for OT systems, especially relating to aging legacy assets created before cybersecurity was an issue. Some asset may have had internet connectivity and remote control bolted on later without regard to security.

3

Establish the budget and risk profile

The next step is for the hospital management to make the OT security part of the overall cyber security strategy. This should include the development of a new OT security policy and conducting a comprehensive risk survey, overseen by the cyber team and led by the CISO. If there's no CISO, it may be necessary to hire in a third-party cyber service provider with specialist knowhow in protecting OT networks. But whoever's carrying out the work, the communication channel to the board needs to remain open throughout, to sustain top-level commitment.

4

Progress to the implementation stage

The risk survey provides the insights needed to develop and roll out a long-term roadmap and an implementation program. Actions should be prioritized based on scale and potential impact of the risks being mitigated, the speed at which they can be implemented, and the costs of doing so. It will often be possible to pinpoint linkages between critical operational systems and other OT assets that are currently unsecured. In cases where a successful cyberattack exploiting these linkages could put lives in danger, these risks should be prioritized.

Maintaining OT security into the future

Effective cyber security controls – whether for OT or any other asset – must include all three elements of the 'PPT': processes, people and technology. Failings to address any one of these three will leave OT systems exposed and vulnerable. And in order to maintain effective defenses, it's vital that all stakeholders recognize the need for proper planning around security when installing new control systems or dealing with old ones, and take a holistic view of OT assets and the potential impact if something goes wrong.

In its reliance on PPT, cyber defense in an operational environment is not actually all that different from addressing any other threat, such as physical sabotage, electric short circuits, fire or water leakage. A hospital gas room without a fire sensor and extinguisher is of course unthinkable – so it would be a natural step for hospitals to embed a similar mindset for cyber monitoring and defense mechanisms into all hospital's OT assets. This is not just desirable, but – in our view – imperative. It's the long-term future PwC should aim to bring about.

Building a 'cyber-hygiene' culture

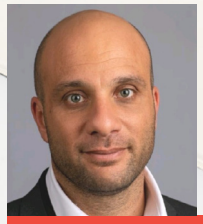
To truly address cyber threats to both OT and IT, hospitals should look to develop and embed a culture of digital safety and security. This should echo the culture of physical hygiene that is second nature to anyone working in a hospital.

Contributors

Rafael Maman

PwC Israel
Partner

Office: +972 52 358 9008
Email: rafael.maman@pwc.com



Gilad Zinger

PwC Israel
Senior Manager

Mobile: +972 50 827 6400
Email: gilad.zinger@pwc.com

Petr Spirik

PwC Czech Republic
Director

Office: +420 774 191101
Email: petr.spirik@pwc.com

Joerg Asma

PwC Germany
Partner

Mobile: +49 160 6142945
Email: joerg.asma@pwc.com

Dr. Benedict Gross

PwC Germany
Senior Manager

Mobile: +49 151 1432 5832
Email: benedict.gross@pwc.com

2020-10-19_RITM3915098