DIGITAL INFRASTRUCTURE ADVISORS LTD

# Data Centre Operational Technology

# An Overview of Cyber Threat

The following article provides an overview of the Cyber threat facing Data Centre operators through real and present vulnerabilities and the preeminent risk to their critical facility networks.

By Mike West // Digital Infrastructure Advisors // May 2021

## What the Data Centre stakeholder needs to know about overlooked Cyber Security risks already prevalent elsewhere throughout industry

For those with a significant stake or role in a Data Centre business, whether it's for their own organisation or for others, here is a burning question:

**'Does the Cyber Security for your Data Centre Operational Technology get overlooked because it falls between your IT, Security and Engineering teams?'**

Throughout industry, Industrial Control Systems (ICS) have long been targeted with Cyber Crime. Now, however, more malicious, and sophisticated strains of Malware and Ransomware are specifically targeting Operational Technology (OT) environments. As the Data Centre industry develops, forward-thinking operators are using techniques and approaches typical of more complex industrial facilities to drive innovation.

It is time to reclassify the Data Centre Operational Technology (DCOT) environments, ensuring they are treated separately.

## The risks for Data Centres are growing

Data Centre stakeholders should be seriously concerned about the impact of Cyber Attack on their DCOT, an impact which is compounded by a combination of downtime and severe financial hits.

Dan Coats, the US director of National Intelligence warned of the danger of a crippling Cyber Attack in a speech in 2019, drawing a parallel with the increased Cyber Chatter detected amongst terrorist groups ahead of the World Trade Centre attack in 2001.

**"Here we are nearly two decades later, and I'm here to say that the warning lights are blinking red again. Today the digital infrastructure…is literally under attack."**

## Downtime through Cyber-attack is unthinkable

In the Data Centre Industry, downtime is measured in seconds, minutes and for a serious outage, hours. When it comes to recovery from a Cyber breach, though, it is measured in days, weeks, and months – a totally different landscape.

Financial impacts are similarly compounded. The Uptime Institute reported that one in ten major outages at a Data Centre costs over £1m, and cited examples of substantially greater financial impact.

It is clear, however that the average cost of downtime is dwarfed when we start to look at the costs associated with a Cyber breach. In April 2020, IT services and Data Centre provider Cognizant was hit by a ransomware attack that, it forewarned investors in July, could cost it between $50m and $70m.

Data Centre owners in countries such as the UK are mistaken if they think it is really only US companies that are at risk; this is not true. Whilst the US has most attacks and suffers the highest losses, in the UK the average loss was slightly higher than the global average of $3.9m.

And research shows that Data Centres are at a particular risk, with the average loss to a technology company being much higher than the average, standing at $5.04m, the fifth most 'at risk' industry after Healthcare, Energy, Financial and Pharma.

Mike West, CEO of Digital Infrastructure Advisers, a company specialising in Data Centres asks, "Do you see the Cyber threat being a risk for your customers' or your company's data rather than for you, the building operator?

"As a building operator, it's your Operational Technology that is at risk. There are scores of vulnerabilities in and around the Data Centre facility itself, where increasingly clever hackers are able to get in and cause devastation, and where there is grave doubt that you are protected."

Mike explains: "Your DCOT comprises all the equipment and services embedded in your building, from your biometric, security and CCTV to your critical power and cooling, Internet of Things (IoT) devices and sensors, fire & life safety systems, remote monitoring tools, building management systems as well as control systems on multiple networks, which have many protocols and platforms such as BacNet, ModBus, SCADA, TCPIP, Distributed Control Systems (DCS), Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC).

"These terms are well-known and catered for throughout major industries, but they are still not widely recognised in the world of Data Centres. "The equipment that keeps your building running is very similar, if not the same, as the equipment that keeps a Power Station or car manufacturing plant such as Honda going.

"Exactly as in these industries, your building's equipment will be at least partly maintained and serviced by external suppliers. They employ people who come in from outside with laptops, tablets and phones, and log naively into your systems, just doing their jobs. Increasingly, thanks to IoT, they maintain your systems remotely."

Mike argues that the Data Centre operator is not only responsible for their own building's security but are suddenly at the mercy of their security. He says, "You might be right in thinking that this area is beneath your notice, but your own DCOT is bringing a potentially devastating threat right there, beneath your nose."

## The burgeoning costs of Cyber-crime in the Data Centre world

Where a ransom demand is made, it is only the start of the financial cost of a Cyber Attack. In the well-documented Equinix case for example, attackers reportedly asked for $4.5m USD, but the additional financial consequence of this attack and the potential unseen long-term effect on its business were much greater.

To ransoms and operational recovery costs may be added the severe fines imposed as a result of subsequent regulatory investigation. For example, the EU GDPR sets a maximum fine of €20 million or 4% of annual global turnover – whichever is greater – for infringements. This type of regulation is already extending beyond personal data theft, and considering the impact to safety and disruption to national critical infrastructure.

Our connected world has become a lucrative playground for criminals who can launch attacks on victims in multiple countries and jurisdictions, with little fear of being caught.

Cyber criminals steal an estimated $600 billion per year from governments, companies, and individuals, while the overall loss of company revenues over the course of five years from 2019 to 2023 will reach $5.2 trillion. In fact, Cyber-crime is one of the most disruptive and economically damaging criminal activities in the world today.

## Supply chain attacks which include the SME sector

Whilst those in Data Centres are fortunate enough to be working in a growing industry in that Data Centres are now essential to the fabric of society, and one of the foundations of our increasingly digital lives, we must recognise that an attack on the Data Centre infrastructure is an attack on all the businesses it supports, irrespective of the size, scale, or location of the facility.

This isn't about data security, it's about being a core component of the technology supply chain, which increasingly contains SME's as well as major corporates. Data Centre operators could be forgiven for thinking that it's the larger companies that are at risk of Cyber Attack; this simply is not true. Mid-sized organisations are essential components in any supply chain; they experienced the biggest increase in average breach cost, and smaller organisations had higher than average costs per employee. These are possibly the organisations that have taken fewer steps to protect themselves.

As an example, the UK MOD's Small and Medium-sized Enterprise Action Plan 2019-2022 aims to spend 25% of its £186b budget away from its 19 Strategic Suppliers, and with SME's, bringing a considerable number of additional players into the Cyber attackers' crosshairs.

"The biggest loss to a Data Centre in the end, is that of trust," says Mike West. "If the very company that houses its customers' precious IT assets, has allowed a data breach in its own systems or facility infrastructure, the resultant loss in confidence can be difficult to recover from. With technology companies standing to lose more than the average in terms both of money and reputation, it is not a situation that a responsible stakeholder can ignore."

The widely-reported SolarWinds attack clearly demonstrates the impact of a supply chain strike, and how Cyber gangs are becoming more sophisticated in approach as well as in the use of technology. No doubt there is more to come from this incident because it highlights the disastrous and widespread impact of embedded Cyber infection or hacking at source.

## Why Data Centres may not be 'the most secure facilities in the world'

Whilst some may hide behind the veil of physical security, (certain Data Centres mention being 'the most secure facilities in the world', with sophisticated multi-layer protection zones and high-end systems), ironically the IoT devices used on these networks can be used by Cyber criminals to get access to the broader DCOT network.

We are all aware of the almost unthinkably destructive actions a malicious insider could take, but perhaps the real risk is latent, hiding in the code of an electronic IoT device, waiting to be activated, as the hack on the Schneider Triconex Safety systems demonstrates. In this incident, the hackers' software gave them remote control over the plant's safety instrumented systems, designed to defend against life-threatening disasters.

As the sophistication of the Data Centre infrastructure develops, and many smart building techniques integrated with control and automation systems are adopted, there is further risk that attackers will use evermore imaginative ways to find a back door even to the most highly secure, so-called 'dark' sites.

With so many engineers, from both operator and client teams, entering the facilities with uncontrolled hardware, and the prolific use of IoT devices and out-of-band network facilities on plant and equipment, a clear plan of defence measures have been compromised.

Our world is now about novel and new Cyber Attacks and never-before-seen events, and so the landscape has become massively challenging for security teams to defend. With low and slow, hard-to-detect techniques, through to machine speed attacks, where criminals weaponize AI, it is clear that human speed responses are no longer adequate.

## Cyber criminals are taking an ecosystem approach

Cyber-crime is becoming ever more lucrative, and we are seeing Cyber gangs operate in concert, using Ransomware-as-a-service from the dark web, to conduct malicious attacks at scale, as the widely publicised case of WannaCry demonstrated; it is clear that traditional security approaches are inadequate.

Of all the types of crime, Cyber continues to increase at the fastest rate. According to INTERPOL, as quoted within the World Economic Forum (WEF) Future Series:

**"'Cybersecurity, emerging technology and systemic risk', is an insight report published in November 2020, citing 'In less than a decade since cybersecurity first featured in the Global Risks report, it has emerged as one of the most important systemic issues for the global economy."**

## Solutions for Data Centres to consider

The WEF report comes to three conclusions, the third of which is Leadership action: “Business leaders need the ability to plan more strategically for emerging risk, so they can ensure that the organisations delivering the most critical infrastructures do not suffer failures that are catastrophic for societies.”

Mike West agrees. “Given the Data Centre industry is a strategic part of the world’s technology infrastructure, and Industry has demonstrated high levels of collaboration tackling key challenges, there is no doubt that Cyber resilience and security are a shared responsibility that involves everyone and, as such, require an ongoing holistic, systematic and coordinated approach.”

## Decide where the responsibility lies for the Cyber risk at DCOT level

Because the infrastructure in a Data Centre is focused on keeping the computers going, there is usually little or no focus on the security around the Operational Technology. Mike West asks:

“Whose responsibility are these networks? Is it the engineering department because it’s to do with the mechanics of the building? Is it the IT department because it’s got Cyber written on it? Or it is security because they are in charge of protecting the building? This question must be answered at the top, where the key stakeholders sit.

“It’s an abnormal, overlooked risk and if you are leading a Data Centre business, it’s time you got involved. You need to ensure it’s clear where the overall responsibility for your systematic, coordinated approach lies.”

## Don’t be tempted to kick this can down the road

The threats to a Data Centre business via its Operational Technology is urgent, and whilst it’s understandable to consider this as a problem that can be dealt with ‘later’, it is alive and ready to kick right now.

Mike West says, “We would argue that Data Centres are amongst the most critical infrastructures in society, because the data held in these facilities is increasingly vital to the way communities run. Tomorrow is too late to start looking at the risk to DCOT, which underpins the facilities.”

Data Centres are used to support utilities, hospitals & healthcare, food manufacturers, the logistics and transport industries, education, defence, and communications – all examples of key sectors that affect the very fabric of how the world runs.

## Consider specialist Data Centre Operational Technology Cyber protection

Mike West has spent his career in Data Centres, and his company, Digital Infrastructure Advisors, has a unique awareness of where and how this new threat can devastate not only the Data Centre business, but also that of its customers. The organisation’s deep knowledge of how Data Centres are built, how they operate and how they are maintained means

that they can see things that most people overlook. Its Data Centre advisory and technical services extend to specific Cyber services including compliance, audit, testing and technology solutions.

## An opportunity to take protective action against Cyber in the DCOT

Digital Infrastructure Advisors has partnered with one of the world's most powerful providers of Cyber AI security, and the creator of Autonomous Response Technology, Darktrace.

Because Darktrace's AI technology doesn't look at yesterday's attack to predict that of tomorrow, it has the unique ability to find potential threats that have never been seen before.

Every three seconds, Darktrace AI fights back against a Cyber-threat, preventing it from causing damage.

With Digital Infrastructure Advisors' intimate knowledge of the potential risks to Data Centres and specifically their Operational Technology, the partnership between the two organisations is a powerful ally to the Data Centre stakeholder.

The Darktrace technology with Digital Infrastructure Advisors' insight is uniquely positioned to support both the Industrial and DCOT environments as well as corporate networks including cloud, SaaS, and email, providing a single unified platform to protect 'every corner of the network' for Data Centre business from Cyber threat.

## Proof of value to the Data Centre

As a way of enabling organisations to carry out due diligence on this collaborative solution, Digital Infrastructure Advisors and Darktrace have developed a complimentary 'Proof of Value' opportunity for Data Centre operators.

Because of the self-learning nature of the technology, there is very little configuration needed, and it may be set up in under one hour, during the 30 day process you will benefit from: -

- Unique insight into your network and connected devices
- Hands on interrogation of your network through the initiative Dashboard
- Live reporting on network vulnerabilities, anomalies, and potential breaches
- Allocated Cyber Technologist
- Three Threat Intelligence reports on your network
- Building common understanding and learning amongst the operational teams
- Complimentary and no obligation

For further information on our Data Centre Advisory and Cyber services or to set up your complimentary trial, please contact mike.west@dia.ltd or call +44 (0) 7768 557 191

**https://www.digitalinfrastructureadvisors.com/**

## Case Study: Protection against one of the world's most notorious Cyber Attackers

Shamoon is a highly destructive malware, which has been associated with the interests of the Iranian state. Shamoon 3 is so called because it seems to be a new version of the malware.

At a global energy company, Darktrace's Industrial Immune system detected Shamoon 3 in its earliest stages, flagging the threat to the security team as soon as it detected the initial intrusion. Read more about this incident, and the indicators of compromise that most likely represent lateral movement activity in the weeks prior to the 'detonation'.