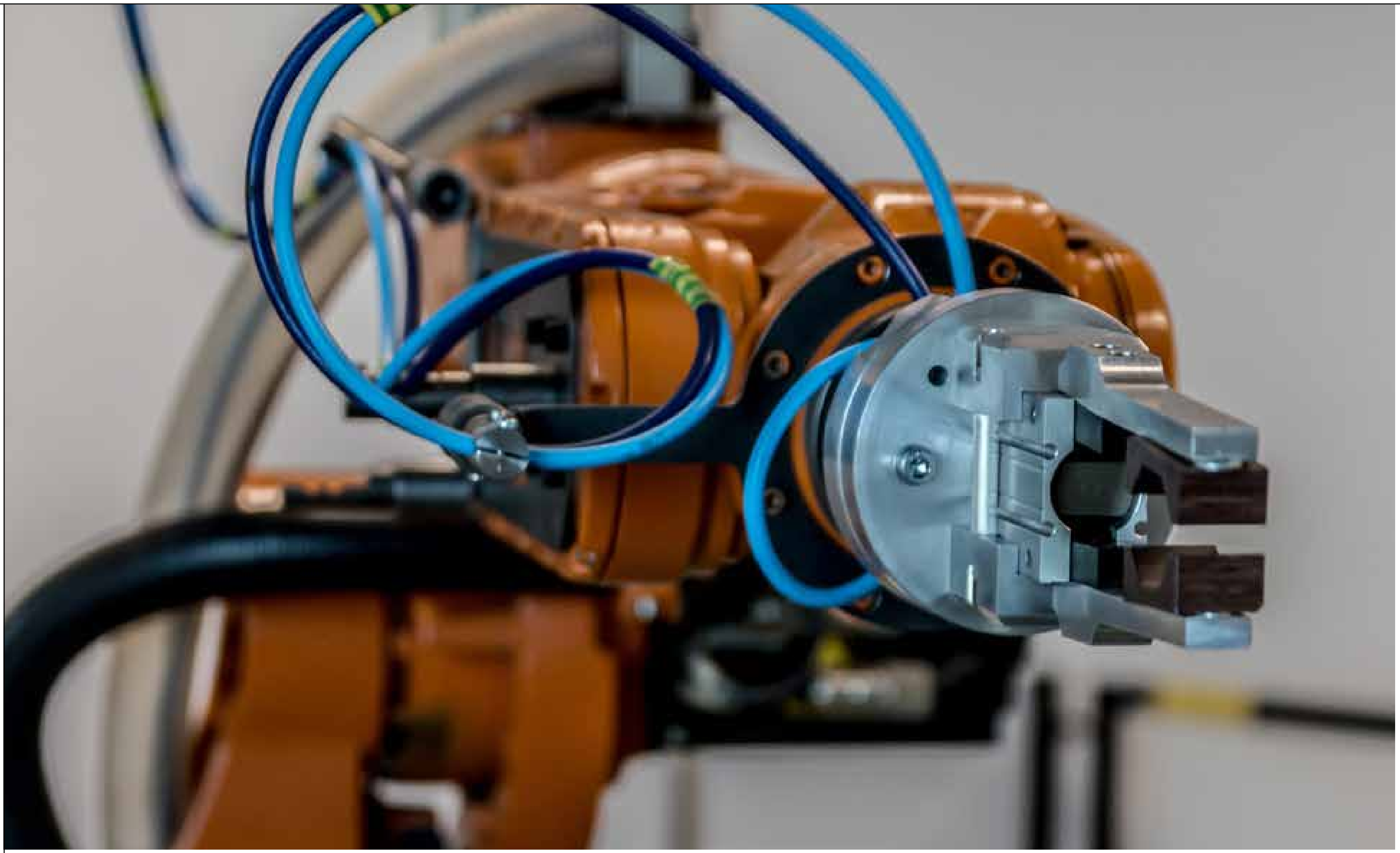

DIGITISING INDUSTRY

Grant Geyer *examines the difficulties involved in balancing the risks and rewards of the digital enterprise*

Digital transformation has enabled tremendous competitive advantages for the modern enterprise, and not surprisingly has come to dominate the business agenda in recent years. IDC estimates that $2.3-trillion will be spent globally on digitalisation projects in the next four years – accounting for more than half of all IT spending.

The benefits of digital transformation are well documented, including improving operational efficiency, enhancing customer outcomes, as well as opening up entirely new business models and disrupting legacy markets in some cases. Additionally, the enormous changes wrought by the COVID-19 pandemic have served as a case study into how valuable a digital operation can be, with those companies with more advanced digital infrastructure having a much easier time of adapting to the new normal of remote working.

However, these operational benefits are offset by an increased exposure to digital risks – and chief among them is cyber security. More digital infrastructure and interconnectivity means a greater surface area that can be potentially exploited by threat actors, as well as more potential impact if a breach occurs. Businesses must perform a constant balancing act between implementing new digital initiatives and modernising their operations, and ensuring they are taking steps to mitigate potential new digital risks.

The challenge is to connect OT systems to traditional modern IT networks while also keeping them secure

Perhaps nowhere is this more true than in sectors that rely on operational technology (OT). These systems, which control and monitor a wide variety of machinery, are very distinct from traditional IT systems and digitising them securely can present some significant challenges. However, these sectors are under increasing pressure to reap the rewards of the digital economy in order to remain competitive.

Digitalisation has been a major priority in most industrial sectors for several years now, with many elements undergoing a seismic shift in operational structure. The development has been compared with the industrial revolutions of old. Indeed, the phrase "Industry 4.0" was coined by the German Government in 2011, along with the "Fourth Industrial Revolution" a few years later by the executive chairman of the World Economic Forum. Connecting industrial equipment to digital control systems creates a whole new world of possibilities for automated operations, such as predictive maintenance, just-in-time ordering and manufacturing optimisation. Looking ahead, many governments and corporations are making grand plans for smart factories, energy production, and even entire smart cities.

However, there is a stark difference between planning for an entirely new breed of digital industry and successfully digitising existing infrastructure. Manufacturers, energy producers and others are not at liberty to simply replace their entire operation with new technology and must find a way to integrate their existing infrastructure if they want to keep up.

This means overcoming the fundamental challenge of connecting OT systems to traditional modern IT networks to reap the digital rewards – while also keeping them secure against exploitation by threat actors.

There are a number of factors that make OT difficult to secure in a modern digital environment. Most OT networks run on legacy equipment with proprietary protocols that are completely incompatible with standard enterprise IT environments. Industrial equipment is built to last, often with an intended lifecycle of many years or even decades – and the OT systems behind them are designed to the same time scale. This stands in stark contrast to the mayfly existence of modern software, which is continually being updated or replaced with the next version. Equipment such as engineering stations and human machine interfaces (HMIs) often has a refresh cycle of around five to 10 years, which means the underlying operating system will be vastly outdated by normal IT standards.

These differences make secure interconnectivity between OT and IT different, but not impossible. For example, the Programable Logic Controllers (PLCs) running most OT processes aren't built for endpoint protection.

With the right approaches, connecting an OT environment to the IT network means introducing an operating system that might be nearly old enough to vote, with no means of patching its vulnerabilities. Mitigating the inherent risk requires a different mindset and approach.

The main reason OT systems are so wildly insecure by normal IT standards is that they were largely built for a very different world with different priorities. OT systems are usually built to the 'CIA Triad' – confidentiality, integrity and availability. Availability or uptime is more important than confidentiality and data security for OT systems, as downtime in critical infrastructure can be catastrophic and even lead to loss of human life. As a result, it is not feasible to shut down many OT systems for maintenance, even temporarily. In stark contrast, with IT systems, data confidentiality and security maintain equal footing with uptime and IT teams must regularly account for planned downtime for maintenance such as security updates.

Instead, OT systems were built with process safety, process integrity and process availability in mind. The process *is* the business and if it isn't running the enterprise can't deliver value.

OT SYSTEMS ARE INSECURE BY IT STANDARDS BECAUSE THEY WERE BUILT FOR A VERY DIFFERENT WORLD

Even as IT systems developed around them, the mindset of protecting OT assets was based on a policy of 'security by isolation'. If the OT and IT networks do not intersect and have a complete air gap between them, there is no way for a threat actor to jump from one to the other. However, an air gap is just a very low latency network. As the business needs efficiency to operate, people will work around barriers that inhibit their ability to operate.

As a result, this mental model fails in the face of digital transformation and no longer makes sense once OT systems are connected to the main network as part of automation efforts. Sophisticated cyber criminals will be quick to identify and exploit vulnerabilities as OT systems are brought online. Because OT generally controls and monitors real-time processes relating to essential industrial equipment, any level of disruption from a cyber attack could have disastrous consequences, representing a very real physical threat as well as a digital one.

In addition, OT networks often have limited bandwidth, so attempting to scan for vulnerabilities can disrupt their operation, resulting in unplanned downtime that few industrial settings can afford.

While the distinct differences between IT and OT present significant security challenges, these can be overcome by deploying a security solution that is designed specifically for the idiosyncrasies of an OT environment. Security solutions must account for a number of different key factors:

ESTABLISHING VISIBILITY

The first step to addressing any form of cyber threat is proper risk assessment. For OT systems, this must address three key areas: assets, network sessions and processes. Achieving this requires full visibility into the OT assets, architectures and protocols. This means a solution must be able to account for the myriad of different proprietary protocols present across different assets, as well as scanning and providing remote access in such a way as to not disrupt the tenuous bandwidth afforded by most OT networks.

▶

Once this has been achieved, it will be possible to start detecting and remediating active threats, as well as carrying out more long-term strategic security planning.

DETECTING & MITIGATING THREATS

Speed is of the essence when it comes to fighting any form of cyber threat. Attacks such as ransomware can spread through the system extremely quickly, while attempts to infiltrate the network and access classified information must be stopped early on before the threat actor can escalate their privilege.

The need for speed is particularly pressing when it comes to defending OT. Even a brief disruption to an industrial control system can cause an entire factory line to grind to a halt and rack up millions of pounds of costs, for example or disrupt power supply to thousands of homes and businesses. As such, security solutions will need to be able to identify threats in real time, accounting for both known threats with recognised profiles and suspicious activity that points towards a previously unseen zero day.

Mitigation can be further accelerated by automatically grouping related alerts together, producing a higher signal-to-noise ratio that means significant threats are less likely to be missed against the constant hum of false positives. This also makes it easier to identify the subtle signs of malicious activity across multiple systems that may point towards an advanced attack in progress. Security teams need to have a unified view of the threat landscape across both IT and OT networks simultaneously.

VULNERABILITY MANAGEMENT

Alongside detecting active threats endangering the network, it is also important to continually identify and reduce risks within the industrial environment. The fact that OT networks are generally made up of legacy equipment dating back many years means there is usually a high volume of potential vulnerabilities to account for. However, there is also a high number of false negatives and positives to contend with, thanks in part to the restrictions imposed by limited operational bandwidth.

These challenges can be overcome by automatically identifying and comparing individual OT assets to a database of known vulnerabilities, including various sources such as the latest Common Vulnerabilities and Exposures (CVE) data from the National Vulnerability Database (NVD).

Following this, security teams will need to prioritise the vulnerabilities that pose the biggest threat to their unique operational environment, while also quickly filtering out the background noise of false positives.

Digital transformation and Industry 4.0 have already dominated the industrial agenda for some time now as organisations seek to modernise and improve productivity and profitability – as well as keeping up with more agile rivals. However, businesses must also now contend with even more pressure due to the COVID-19 pandemic.

The pandemic and accompanying mitigation strategies deployed around the world mean that possessing a digital, remote capable operation has transformed almost overnight from a competitive advantage to an essential asset for continuing to operate. While lockdown measures have eased in some countries, remote work is still strongly encouraged where possible, and firms must also plan for the possibility of future outbreaks and additional preventative measures.

While most industrial settings are incapable of deploying a fully remote workforce, it will still be highly advantageous to be able to reduce onsite staffing levels when needed. Achieving interoperability between OT and IT systems is an essential part of enabling teams to perform their duties from a remote location. However, while organisations must move swiftly to prepare their OT assets for digital connectivity, they must also ensure they have the right specialised tools to detect and defeat the accompanying cyber threats ●

Grant Geyer oversees Claroty's product management, engineering, and research organisations, and is responsible for the company's product strategy and development. He has had a successful career as an operator in the cybersecurity industry for over 20 years.

Most OT networks run on legacy equipment with proprietary protocols that are completely incompatible with standard enterprise IT environments