Picture credit: Carolinebn8

Industroyer was designed to affect ICS systems used in electrical substations and used as part of the conflict in Ukraine

PROTECT YOUR WEAK SPOTS

Paul Baird *provides essential advice on the best way to link your operational and IT security together*

IT security is big business. Gartner predicts that spending on information security products and services will grow by 11.3 percent in 2023, reaching more than $188.3-billion globally. But while the approaches around IT devices, cloud computing services and IT networks have grown massively, there is an area that is lagging behind significantly – operational technology that companies use to run their physical infrastructure.

Operational Technology, or OT, includes all the IT systems used to manage areas like manufacturing systems, production lines and industrial processes. NIST defines OT as: "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information". Typical applications include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

In the past, OT networks were kept secure by running them on separate networks that were not connected to other systems, otherwise known as air gapping. However, this approach is no longer possible or desirable. Companies want data from their OT systems to make decisions in real time, rather than waiting on data exports or reports that are out of date as soon as they are compiled. This requires implementing systems using the Purdue Reference Model, where ICS systems and their programmable logic controllers (PLCs) run at level 1 and 2, then enterprise applications run separately at level 5 through a demilitarised zone, or DMZ. Each level should have security measures like firewalls between them to stop unauthorised traffic.

Having access to data faster helps businesses run more efficiently and trade more effectively, which is essential in today's modern global and interconnected economy. However, this means more connectivity is needed, and the air gapping model is not possible. According to the Dragos 2022 ICS/OT Cybersecurity Year In Review report, about half – 53 percent – of all ICS and OT systems now have external network connections. However, this opens up these systems to potential attack without the correct cyber security governance in place, which traditional IT networks have been following for years .

Because these systems were not connected to external or public networks, security could be overlooked when it would affect business operations. While modern IT systems developed to cope with real-time security issues and huge volumes of attacks, OT security approaches are less likely to have kept pace. According to Dragos, 80 percent of companies have little to no insight into their OT networks.

This is the basic requirement for all effective security planning – after all, you can't secure what you don't know about. While companies should be aware of everything attached to their OT networks, there is a difference between what you think you have in place and what actually is connected. On the IT side, common metrics used include tracking the percentage of assets that are managed versus unmanaged, and how up to date the software is on those assets. While 100 percent accuracy is the goal, 97 percent accuracy is seen as 'good'. Maintaining this level of accuracy as devices move in and out of the network or require patches is where the hard work takes place.

For OT assets, this level of accuracy should be the goal too. For very large assets, like physical plant machinery, you may think it is impossible to miss whether they are on or off the OT network. However, these systems will have multiple interconnected components. A lot of this OT equipment will also be directly connected to IT assets so that staff can interact or carry out management tasks too.

Checking which assets are connected can throw up some surprises, from the assets that you did not consider, that were connected without your knowledge or that had been left in place rather than decommissioned. Without that insight in the first place, you leave yourself open to potential attacks over time. Lacking this OT asset overview makes it impossible for you to truly say that you have a full picture of what is in place, how protected those assets are, and how you are prepared to keep security effective over time.

In order to improve OT security, you will have to bring your processes up to speed around areas like asset management, patching, network segmentation and threat intelligence analysis. These processes have developed quickly in the world of IT based on the volume and variety of attacks taking place.

There are more threats to OT systems than ever before. For example, security researchers have discovered approaches to move within OT networks and take advantage of issues in their implementations of networks that are equivalent to Purdue's Layer 1. ICS systems are targeted with specific malware to damage components. A good example of this is Industroyer, which was designed to affect ICS systems used in electrical substations and used as part of the conflict in Ukraine.

The malware landscape has evolved with new malware like INCONTROLLER aimed at ICS systems more generally through their programmable logic controllers and with a fully fledged framework for accessing devices, download and upload files, and exploit specific vulnerabilities in those devices. These customised malware developments point to more effort being put into attacks on OT networks, and work through misusing common standards like CODESYS to carry out functions as well as attacking existing security issues in order to work.

To prevent these kinds of attacks from succeeding, there are multiple steps to take. Implementing better access-control and authorisation mechanisms can help reduce the ability for bad actors to get onto the network in the first place, while restricting access can prevent mis-use of industry standards like CODESYS. Alongside this, teams need to improve their intrusion detection and analysis capabilities for their OT networks just as they have done for IT networks and cloud deployments. Adding real-time asset detection to the OT network like its IT counterpart will allow for more asset control so no unauthorised assets are left unattended.

GARTNER PREDICTS INFORMATION SECURITY PRODUCT SPENDING WILL GROW BY 11.3% IN 2023

To help in these processes, the Cybersecurity and Infrastructure Security Agency (CISA) has developed a Working Group on ICS to develop more best practices and share information on developments. Standards are improving as well – under the aegis of the International Electrotechnical Commission and the International Society for Automation, the IEC/ISA 62443 series of standards provides guidance on security best practices for OT environments. Specific standards have been developed for patch management in OT environments as well.

Alongside the wider industry development work taking place around standards, there are also changes that you can make internally. Consolidating IT and OT security management under one team can help. Today, many OT and IT teams within companies don't work together on a regular basis causing a lack of understanding on both sides – for example, the IT team would be hard-pressed to tell what is installed on the OT network and vice versa. This has to evolve so that security processes on the OT side can improve and teams can deliver that consistent approach to managing risk effectively. This can ensure that areas like patching get addressed across both IT and OT assets in the same way.

As an example, patching is one of the best approaches to preventing security issues. Applying patches quickly stops attackers from entering networks or gaining a foothold on devices which can then be leveraged to get into high value assets elsewhere. It ties into the overall picture that you can have of your overall IT and OT networks, and the various software packages and operating systems that exist across your estate. However, this is often where the problems come in for those companies running OT systems.

For companies that have to operate 24/7, simply finding the time to implement patches and updates is hard, if not impossible. If you have to take systems down to apply updates, this directly affects revenue for the period when updates are deployed, and there is a risk factor in bringing those systems back online successfully

▶

too. These risks can lead to patches being put off for later, relying on mitigating factors like air gapping to prevent attacks. However, with more OT systems getting connected, this is no longer as reliable as it once was. These OT assets represent high-value targets for attackers, whether these groups are motivated by financial gain or by nation state goals.

CUSTOMISED MALWARE DEVELOPMENTS POINT TO MORE EFFORT INTO OT NETWORK ATTACKS

In these circumstances, the role for security is not just about understanding best practices and applying them consistently. It involves educating the rest of the business – and particularly the leadership team – around how important a strong security programme across both IT and OT is. While many boards at companies now recognise the importance of security, they will have to understand the issues that might come up around stopping production systems to apply updates and the risks that arise if these activities don't take place. Would they rather have a controlled outage for a system update or an uncontrolled outage from a bad actor accessing internal systems?

Boards and business leaders are always told that their primary responsibility is to their shareholders. This normally gets translated into looking at revenue, so any activity that might affect the business in that regard will be discounted or overlooked. However, both boards and executive leadership teams are now more understanding of IT and security risks that can affect their companies around operations. Gartner has predicted that 50 percent of C-level executives will have performance requirements related to risk built into their employment contracts by 2026. This means that management teams have to consider the long-term impact from their decisions and how to deliver resilient and sustainable success over time, rather than just looking at the financial performance for that quarter.

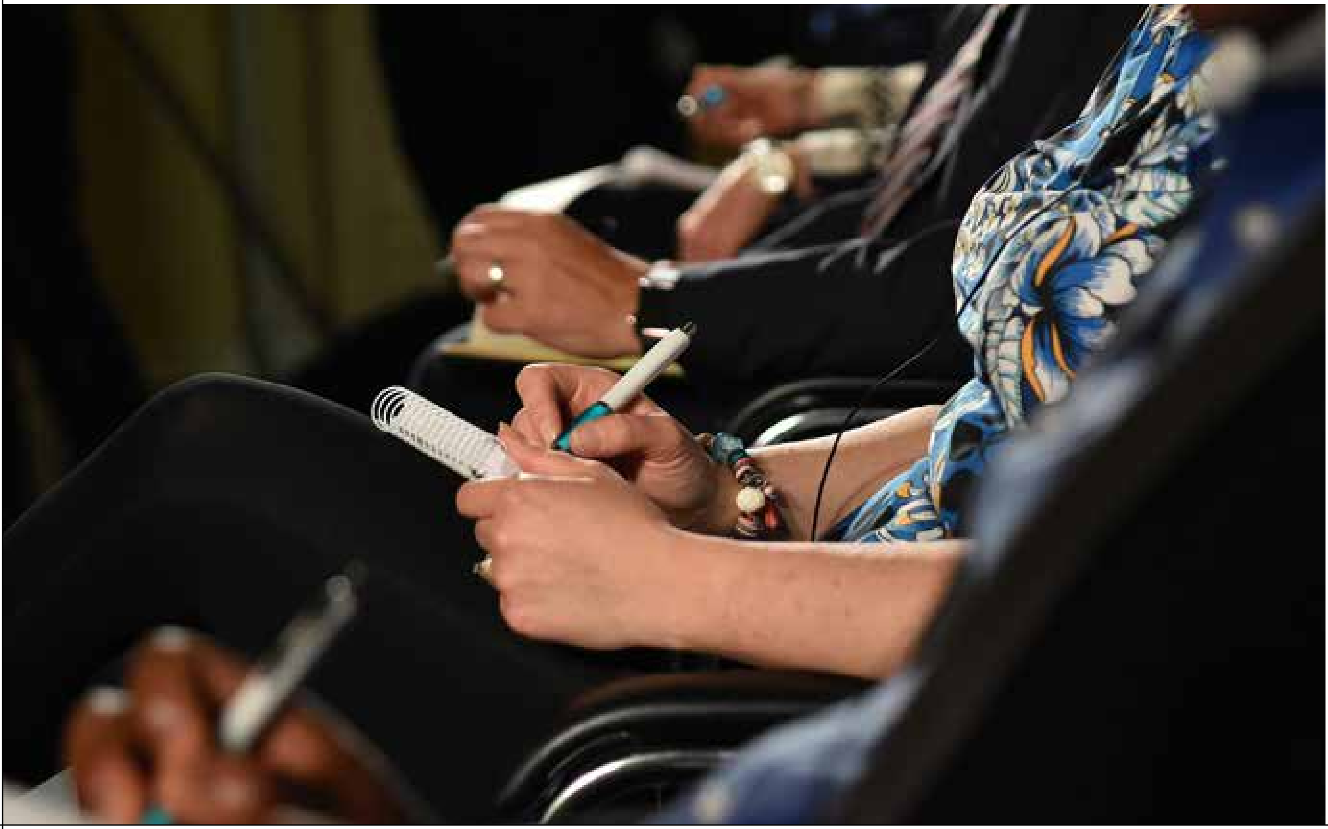
With more skin in the game for these teams, any initiatives that can protect against attack will get more consideration. To succeed here, you can develop metrics to help your board and leadership team understand the level of risk that the business faces alongside the impact from taking time out to carry out updates. This information will help executives measure short-term effects against the potential losses from attacks. There are plenty of examples of the impact of poor security for businesses and organisations that rely on their ICS and OT systems, from Colonial Pipeline and water treatment plants in 2021 through to attacks on companies in the automotive manufacturing, renewable energy sector, electronics manufacturing and oil and gas industries during 2022.

This can be used to provide real-world insight and context on the costs involved in attacks, compared with any losses in productivity. With this data, you can support your approach to maintaining and prioritising security issues and win backing for any planned downtime that is needed. Alternatively, you can make the business aware of what steps are needed and any mitigation measures and costs that are required to maintain services as they are.

In order to make security work more effectively across IT and OT and to protect your most sensitive assets, you have to structure your approach to processes like applying updates and make them part of that wider approach to managing risk. While there are new threats developing that specifically target ICS and OT systems, you can apply some of the best practices developed for IT security to prevent them from affecting your business operations. By building more understanding of risk for the business, you can also get the support you need to ensure that security is managed effectively ●

Paul Baird is a highly experienced and accomplished IT and cybersecurity professional with over 25 years of industry experience. He is the Chief Technical Security Officer for Qualys.

The role for security is not just about understanding best practices and applying them consistently, it also involves educating the rest of the business



Picture credit: Chuck Patch