ELSEVIER

# network SECURITY

ISSN 1353-4858 October 2019

www.networksecuritynewsletter.com

# Featured in this issue:

## Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge

**The convergence of IT and operational technology (OT), especially via the Internet of Things (IoT), presents new risks as well as potential gains.**

The advent of the smart factory and Industry 4.0 represents a new front in the war on cyberthreats. In this hi-tech manufacturing environment, attackers have many opportunities to sabotage and hijack processes as well as steal lucrative data. It's a unique challenge that will demand a response combining best practice security controls, end user education and compliance with industry standards, explains Ian Heritage of Trend Micro UK.

*Full story on page 6…*

## The state of operational technology security

**It's a sad and worrying fact that awareness about cyber security – and subsequent action – has lagged behind as technology has progressed.**

This is particularly true with operational technology (OT). The systems used to run manufacturing plants, control power stations and water utilities, as well as manage countless industrial processes, have often been left poorly protected from cyber attacks. In this interview, Tim Ennis and David Gray of NTT Security discuss the state of OT security and what can be done about it.

*Full story on page 9…*

## Cyber security attacks on robotic platforms

**Robotic technology has been rapidly transforming world economies in terms of business productivity and profitability. However, security threats are not always top of mind.**

Open source platforms, falling hardware and electronics prices and fast prototyping are some of the reasons for this new revolution. Cyber security and physical threats are high-priority areas when critical applications and missions are involved. Dr Akashdeep Bhardwaj, Dr Vinay Avasthi and Dr Sam Goundar analyse the threats to robotic systems and map the CIA model to boost security resilience.

*Full story on page 13…*

## NCSC warns UK universities of cyberthreats

**The UK's National Cyber Security Centre (NCSC) has issued an assessment of the cyberthreats facing the country's universities.**

The report warns that universities are targets for both cyber criminals looking to make money and nation-state hackers engaged in stealing personal information and intellectual property. While the money-seeking criminals may be the cause of the most evident and disruptive activities in the short term, espionage is likely to have greater impact in the long run, the NCSC says. It lists the effects of state espionage as: damage to the value

*Continued on page 2...*

## Contents

**Editorial Office:**
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

**Publishing Director:** Sarah Jenkins

**Editor: Steve Mansfield-Devine**
**E-mail: infosec@webvivant.com**

**Senior Editor:** Sarah Gordon

**Columnists:** Ian Goslin, Karen Renaud, Dave Spence, Colin Tankard

**International Editoral Advisory Board:**
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

**Production Support Manager:** Lin Lucas
E-mail: l.lucas@elsevier.com

**Subscription Information**
An annual subscription to Network Security includes 12 issues and online access for up to 5 users. Subscriptions run for 12 months, from the date payment is received.

**More information:** www.elsevier.com/journals/institutional/network-security/1353-4858



**12987**
**Digitally Produced by**
**Mayfield Press (Oxford) Limited**

*...Continued from front page*

of research, notably in STEM subjects; a fall in investment by the public or private sector in affected universities; and damage to the UK's knowledge advantage.

The kinds of data of interest to nation-state hackers include: emails; bulk personal information on staff and students; technical resources, such as documentation and standards; and sensitive research and intellectual property. How this information is used by the attackers will vary, says the NCSC, but in many cases it is exploited to provide commercial advantage in world markets for attacking nation's businesses. Although the NCSC report names no names, this is likely to be a nod at China.

The report also suggests that universities take a closer look at investment in their institutions. "If foreign direct investment were to come under greater scrutiny or restriction, it is a realistic possibility that the cyberthreat to universities would increase, as nation states sought alternative ways to gain access to sensitive research and intellectual property," it says.

Universities are seen as relatively soft targets because they tend to have an open culture designed to improve collaboration between institutions and academics. "Unfortunately, this also eases the task of an attacker," says the NCSC. The most common forms of attack are phishing and malware.

## US looks to tighten aircraft security

**The US Department of Homeland Security (DHS) has rebooted a programme to discover potential cyber security weaknesses in the aviation sector, as well as strengthen the resilience of critical national infrastructure (CNI).**

According to a recent story in the Wall Street Journal, the DHS is working with the Pentagon and the Department of Transportation to explore whether cyber security vulnerabilities could allow terrorists or nation-state hackers to mount serious attacks on airliners or other aviation systems. While few details have been forthcoming, it's believed the programme will involve some testing on real aircraft.

In 2016, as part of the earlier stages of its aviation security programme, the DHS bought a Boeing 757 and spent over $10m on probing for vulnerabilities. However, the programme got bogged down in disputes over its findings, which included being able to access some aircraft systems via RF communications. Boeing denied some of the alleged weaknesses and the disagreements led to the project being put on hold.

"Improving the cyber security of aviation and, indeed, all areas of critical infrastructure, is an admirable goal," said Jonathan Knudsen, senior security strategist at Synopsys. "However, a stopgap, after-the-fact effort to evaluate security will provide only temporary benefits. To effect real and lasting change in critical infrastructure cyber security, the organisations that create the software products that are used in critical infrastructure must themselves be infused with secure software development practices."

In a separate development, Airbus has revealed that it has been fighting a sustained hacking campaign, mostly targeting its supply chain, according to Agence France Presse. The attacks were on UK engine-maker Rolls-Royce, French tech supplier Expleo and at least two other French Airbus suppliers, says the report. The attackers, believed to be a state-sponsored group based in China, tried to steal technical documentation about the certification process for aircraft systems, as well as documentation relating to the A400M military transport plane and the A350 propulsion and avionics systems. There's more here: http://bit.ly/2OBYo0z.

## FDA issues medical device warning

**The US Food and Drug Administration (FDA) has issued a warning concerning vulnerabilities in software – some of it decades old – currently in use in medical devices and hospital systems.**

All 11 vulnerabilities concern IPnet, a third-party system used to provide communication between computers. While the original developer of IPnet, Interspeak, no longer supports the software, many manufacturers have licences that allow them to build the code into their own solutions.

## Threatwatch

### Android zero-day

A zero-day vulnerability in the Android operating system is being actively exploited by attackers, according to a post by Google's Project Zero. The high-severity issue, which derives from a 'use after free' bug, allows privilege escalation on devices, making them vulnerable to complete takeover. Devices known to be affected include several Pixel models, three Samsung phones and several others – although this is not an exhaustive list. "This issue was patched in Dec 2017 in the 4.14 LTS kernel, AOSP Android 3.18 kernel, AOSP Android 4.4 kernel and AOSP Android 4.9 kernel," said Project Zero's Maddie Stone, "but the Pixel 2 with most recent security bulletin is still vulnerable based on source code review." There is currently no CVE number for the vulnerability. Early reports linked the exploits to the Israel-based NSO Group, which sells malware to intelligence and law enforcement agencies. However, the company has denied any connection. There's more here: http://bit.ly/30VzlrF.

### Attackers target vBulletin

Hackers are rushing to exploit a critical remote code execution (RCE) bug found in 5.x versions of the vBulletin online forum software. A patch was issued for the flaw (CVE-2019-16759) immediately after a zero-day, proof-of-concept exploit was published anonymously on Securelist. However, someone has also created a script that uses the Shodan search engine to find unpatched sites. The flaw is in how vBulletin handles PHP-based widgets: the software can be tricked into running arbitrary widgets via an HTTP POST request, giving an attacker full control over the vBulletin installation. One payload popular among attackers affects password validation, giving the malicious actor persistent access to the site. Tenable has useful information here: http://bit.ly/2AQSxwf.

### Another Exim bug

Another serious flaw has been discovered in the Exim email server. The heap-based buffer overflow bug (CVE-2019-16928) allows remote code execution (RCE) in Exim versions 4.92 to 4.92.2. The buffer overflow occurs when an attacker sends a long string in an Extended HELO (EHLO) Extended Simple Mail Transfer Protocol (ESMTP) command message. The patch was simple but it's important that users update as soon as possible. Debian and Ubuntu have already included upstream patches in their repositories. This follows close behind an earlier vulnerability (CVE-2019-15846), also an RCE bug, that allowed a remote attacker to run code and commands with root level privileges: that has also been patched. The details are here: http://bit.ly/2VsVa0z.

### Reductor breaks TLS encryption

Kaspersky has warned of new malware, dubbed Reductor, that manipulates a browser's random number generator in a way that allows it to spy on a user's web traffic, even when it is encrypted via TLS. The malware is already being deployed for espionage purposes, says the firm, being used against diplomatic targets in the Commonwealth of Independent States. There are some similarities to the COMpfun malware, discovered by G-Data in 2014, which has been linked to Russian-speaking advanced persistent threat group Turla (aka Snake, Venomous Bear, Waterbug and Uroboros), although Kaspersky says there is no clear link between Turla and Reductor. There's more here: http://bit.ly/2Ms42iO.

The vulnerabilities were first discovered in July 2019 by IoT security company Armis. Dubbed Urgent/11, the flaws were thought originally to affect only the VxWorks real-time OS. However, the FDA has warned that other operating systems used by medical solutions are also impacted. These include Integrity by Green Hills, ThreadX by Microsoft, Operating System Embedded by ENEA, ITRON by TRON Forum and ZebOS by IP Infusion.

In its advisory, the FDA says it, "is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available."

It adds: "Some medical device manufacturers are already actively assessing which devices that use these operating systems are affected by Urgent/11 and identifying risk and remediation actions. Several manufacturers have also notified their customers' consumers with devices determined to be affected so far, which include an imaging system, an infusion pump, and an anaesthesia machine. The FDA expects that additional medical devices will be identified that contain one or more of the vulnerabilities associated with the original IPnet software."

The advisory offers a range of recommendations for manufacturers, healthcare providers, patients and caregivers.

The FDA advisory is here: http://bit.ly/35d4RVs.

## Loss of confidence among compliance professionals

**Compliance and procurement professionals are beginning to lose confidence in their ability to manage third-party business relationships, largely as a result of cyber security concerns, according to research by Dun & Bradstreet.**

The '2019 Compliance and Procurement Sentiment' report claims that worries over cyberthreats and concerns over a lack of the right skills in applying artificial intelligence (AI) means that only 85% of professionals are confident about the effectiveness of risk management within their organisation – 8% lower than the previous survey. Some 84% also forecast a decline in the future effectiveness of compliance and procurement functions.

Not surprisingly, smaller firms are less confident about managing third-party risks than larger organisations.

Chief among these concerns is cyber security, yet almost half (48%) of organisations do not yet incorporate it into their third-party risk management. Even those organisations that have developed an approach to cyber risk have been slow to implement it.

Legal and regulatory compliance is another top priority. However, the regulatory landscape continues to grow larger and more complex and this is playing a major factor in compliance and procurement professionals' loss of confidence. And while more than half of them (53%) believe that AI will improve efficiencies and enhance insight within their compliance and procurement functions, fewer (45%) are not confident they have the right skills in place to make full use of it.

The report is available here: http://bit.ly/35aP09Q.

## Report Analysis


# Bitdefender: Hacked Off!

**Cyber security professionals are profoundly concerned about the vulnerability of their organisations to attack, but are too understaffed and under-resourced to prevent it. And these fears are well-founded, in what is shaping up to be a bumper year for breaches.**

These are among the conclusions of Bitdefender's 'Hacked Off!' study, an annual survey about attitudes among cyber security practitioners. And it paints a fairly bleak picture. Of the 6,000 professionals contacted, more than half (57%) said their organisations had suffered a breach in the past three years and around a quarter (24%) had fallen victim in the first half of 2019. But at least if you've had a known breach, you can do something about it. A more worrying statistic is that, among those organisations that have not suffered an incident recently, more than a third (36%) of their cyber security practitioners believe that they are currently undergoing some kind of a breach without knowing it.

Flying in the face of these figures, however, most practitioners rate their organisations' cyber security posture as very good or excellent (57%) or good (another 24%). It's always a worrying sign when the majority of members of a group regard themselves as above average, particularly when the results suggest otherwise. The suggestion is that the problem is elsewhere – a lack of understanding about security issues among the workforce and poor support from the C-suite in enacting change and bolstering defences.

When it comes to abilities, the mood is not quite so ebullient. Less than a fifth (19%) of practitioners rate their own cyber security skills as excellent, and about the same number (21%) have the same opinion of their colleagues. Once you add 'good' and 'very good' into the picture, the overall attitude is that skill levels are pretty high, even if the number of people with those skills may be inadequate.

This report, though, is not just another litany of hacked companies and skill shortages, which are both familiar enough refrains. It's about how cyber security professionals feel about the situation their organisations face and how they are responding to it. And the overall picture is … not well.

Half of C-level cyber security practitioners confess to being kept awake at night worrying about their organisations' security. Lack of staff and resources are key causes of stress. When asked whether they would be concerned about their readiness for another malware outbreak on the scale of WannaCry, more than half (58%) said yes.

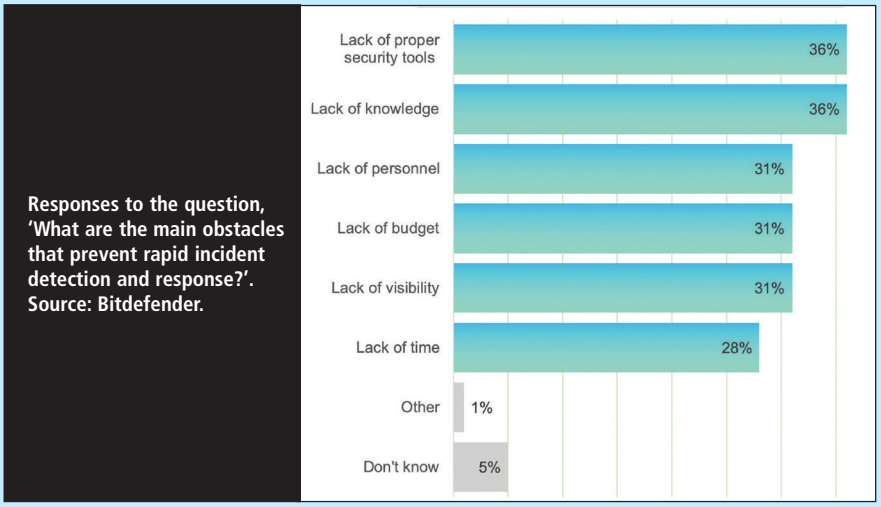
"Resources are such a stressor that 53% of infosec professionals have contemplated leaving their job due to under-resourcing in terms of staff," said Liviu Arsene, global cyber security researcher at Bitdefender. "Resources are in fact such a bugbear that infosec pros say the main obstacles to their organisations' strengthening their cyber security posture are a lack of budget and a lack of skilled personnel."

Alert fatigue is another pain point. Organisations are now more heavily instrumented than ever. The installation of a security incident and event management (SIEM) system is now pretty much obligatory in any firm over a certain size. And endpoint detection and response (EDR) solutions are pretty ubiquitous now – only 4% of the organisations in the survey don't use them. Yet a significant proportion of the respondents cited EDR false alarms at high levels – up to 75%. This creates an enormous extra workload, as well as concern that the time and effort spent dealing with false positives might mask the more dangerous phenomenon of false negatives.

All of this leads to poor responsiveness. Nearly a third of practitioners (29%) reckon it would take a week or longer to detect an advanced cyber attack. Weirdly, the figure is much higher (39%) in organisations that supply cyber security training and support, even though the main reasons given for inadequately rapid incident detection and response are 'lack of knowledge' and a 'lack of proper security tools' (both 36%). Around a third of organisations (31%) reckon they could detect and isolate fewer than half of advanced attacks, and only 3% of professionals believe they can catch all of them. The consequences of failing to detect an ongoing breach were cited as business interruption (43%), reputational cost (38%) and loss of revenue (37%).

"In the last 12 months, cyber security professionals have had to step up their game. As the threat landscape has grown more complex, more comprehensive infosec strategies and solutions have had to be employed to protect business continuity," says Bogdan Botezatu, director of threat research at Bitdefender, in the introduction to the report. "However, there are still gaps. From squeezed budgets and inadequate training to a lack of talent and resourcing, the door has been left ajar for determined cyber criminals to exploit all but the savviest of organisations. Additionally, with the media's continual focus on cyber security failures, organisations which are left exposed to threats could very well find themselves with all the wrong sorts of publicity."

The report is available here: http://bit.ly/2oaLpIp.




**Responses to the question, 'What are the main obstacles that prevent rapid incident detection and response?'. Source: Bitdefender.**

# In brief

### New NSA directorate

The US National Security Agency (NSA) has formed a new directorate aimed at strengthening cyber defences. The Cyber security Directorate is the result of the agency "redefining its cyber security mission", to which end it is unifying a number of existing foreign intelligence and cyber defence missions. The unit will also undertake non-classified collaboration and information sharing with other organisations. "The NSA will work to prevent and eradicate threats to national security systems and critical infrastructure, with an initial focus on the defence industrial base and the improvement of our weapons' security," the agency said in a statement. There's more information here: http://bit.ly/2Vlz9kd.

### CyberPeace Institute

Microsoft, the Hewlett Foundation, Mastercard and a number of other organisations have launched the CyberPeace Institute, a Geneva-based non-profit that aims to, "decrease the frequency, impact and scale of cyber attacks by sophisticated actors that have significant and direct harm on civilians and/or civilian infrastructure". It describes its three core functions as: helping and defending civilian victims of cyber attacks; analysing and investigating cyber attacks; and promoting cyber security norms, prevention of attacks and responsible behaviour. The organisation claims that no other body has the mandate of protecting civilian infrastructure, although how it will go about this is not yet clear. The home page is here: https://cyberpeaceinstitute.org/.

### RDP heavily exploited

The remote desktop protocol (RDP), which is heavily used by organisations for technical support and systems management, is also being widely exploited by attackers, according to new research by security firm Vectra. Its investigation revealed suspicious use of RDP among 90% of organisations using RDP. Over a six-month period, the firm logged 26,800 instances of suspicious RDP behaviour. However, as the firm was monitoring only two kinds of suspect activity, the true scale of the problem could be much higher. Organisations in manufacturing, finance and insurance, retail, government and healthcare are the most likely to be at the receiving end of this kind of attack, Vectra reckons. The report is here: http://bit.ly/2LUkvxb.

### Cyber readiness and mergers

Cyber security standards at organisations can have a profound effect on mergers and acquisition, according to recent research by professional body (ISC)². Its 'Cyber security Assessments in Mergers and Acquisitions' report, which surveyed US-based professionals with mergers and acquisitions (M&A) expertise, looks at how cyber security programmes and breach history factor into the valuation of companies during a potential purchase. Nearly all (96%) of respondents indicated that cyber security readiness factors into the calculation when they are assessing the overall monetary value of a potential acquisition target. And all confirmed that cyber security audits are not only commonplace, but are actually standard practice during M&A transaction preparation. The research also found that the results of such due diligence can have a tangible effect on the outcome of a deal, both in terms of overall value and even whether a deal is completed. The report is here: http://bit.ly/2LSJVLA.

### Russian disinformation

It is "alarmingly simple and inexpensive" to engage the services of Russian cyber criminals in spreading disinformation and influencing Western media, according to new research by Insikt Group. Using the Record Future platform, the firm set up fake companies and then hired 'disinformation vendors' to boost the reputation of one and attack the other. A customised, month-long campaign cost just a few thousand dollars – a social media post, for example, cost $8 while a package of SEO services and media articles was priced at $1,500. Within two weeks, the fake organisation receiving positive mentions was trending and receiving favourable media coverage. There's more information here: http://bit.ly/2VjvEL4.

### WEF top risks

Cyber attacks are still the biggest perceived risk when it comes to doing business in North America and Europe, according to the annual 'Regional Risks for Doing Business' report by the World Economic Forum. Globally, fiscal crises take the top spot, but cyber attacks come in second place and data fraud or theft at number seven. In Europe, "61% of businesses reported cyber incidents compared to 45% in the previous year," says the report. And in Canada and the US, cyber attacks are the biggest concern for organisations "by a large margin". The report is here: http://bit.ly/2LRxYWB.

### ICS attacks

Attacks on industrial control system (ICS) installations have become more probable following the widespread adoption of operational technology (OT) and industrial Internet of things (IIoT) solutions, and nearly all (93%) of security professionals in this field believe that they could lead to operational shutdown or customer-impacting downtime. Two-thirds (66%) believe that a successful attack has the potential for catastrophic consequences, such as causing explosions. These are the findings of a study by Tripwire and Dimensional Research, which also found that 77% of organisations have made ICS cyber security investments over the past two years. However, half of information security professionals still feel that current investments are not enough to counter these threats and many of them (68%) believe it would take a significant attack in order for their organisations to invest more. On the plus side, about half (49%) said that collaboration between IT and OT has improved over the past two years. Typically, it is the IT side of the business that takes the lead on ICS security (44%) compared to OT (14%).

### Firms over-confident about tools

Organisations are placing too much confidence in information security tools, according to the results of a Forrester Consulting study. Typically, companies use a hodgepodge of solutions that provide only 'point in time' visibility into the organisation's security posture. This approach is reactive, labour-intensive and insufficient in scale, says Forrester. This has led to a disparity between appearance and reality, where security decision-makers are being given a false feeling of confidence. Some 86% are confident or very confident that they have no gaps in their security controls deployed across devices, applications, people and data. However, the complexity of today's IT infrastructures and the heterogeneity of enterprise security tools make it difficult for security pros to protect their environments. In fact, 97% experience challenges with their tools because they take a traditional reactive approach to fighting cyber security threats, the report claims. There's more information here: http://bit.ly/2OvsiDp.

### Rise in stalkerware

There has been a rapid rise in the use of 'stalkerware' – commercial spyware that people install on phones to keep track of the devices' users – according to Kaspersky. "The software allows users to spy on other people – for example, to monitor their messages, call information and GPS locations – in complete stealth. It can often be used to abuse the privacy of current or former partners and even strangers," says the firm. In the first eight months of 2019, Kaspersky's monitoring systems noted a 373% rise in the detections of stalkerware, compared to the same period in 2018. This is in spite of the fact that installation of the apps takes some effort – they are not available in official app stores. There's more here: http://bit.ly/2IvUjqA.

# Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge

Ian Heritage

Ian Heritage, Trend Micro UK

**Britain may not be the manufacturing powerhouse it once was. But the industry still contributes a healthy £275bn annually to the national economy, represents 69% of R&D and employs over 2.7 million people.[1] As in other leading manufacturing nations, technology systems are a key enabler of growth. Yet the convergence of IT and operational technology (OT), especially via the Internet of Things (IoT), presents new risks as well as potential gains.**

The advent of the smart factory and Industry 4.0 – which combine these trends in automation with advances in AI, cloud computing and other innovations – represents a new front in the war on cyberthreats. Yet in this hi-tech manufacturing environment, we see not only IT and OT systems but also sensitive intellectual property (IP) presenting attackers with opportunities to sabotage and hijack processes as well as steal potentially lucrative data. It's a unique challenge that will demand a response combining best practice security controls, end user education and compliance with industry standards.

## Network threats

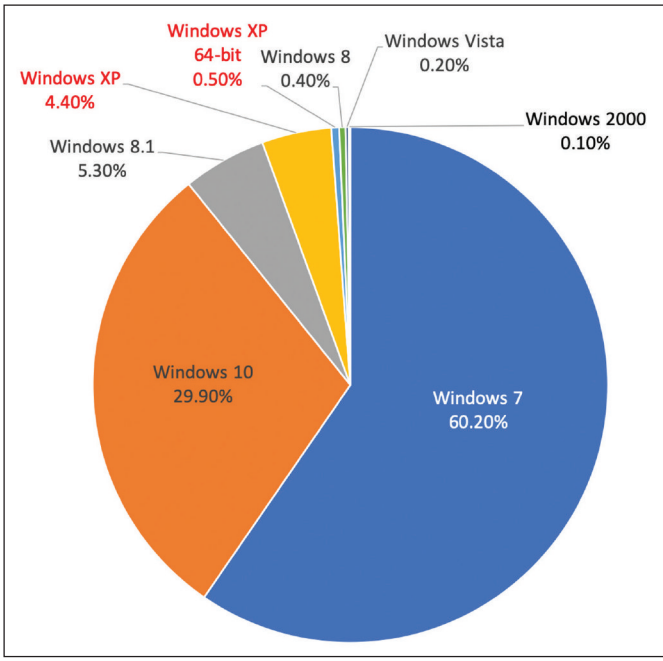
A recent major study of global manufacturing clients compared detection logs with those in other sectors and investigated systemic vulnerabilities to certain threats.[2] The research found that while manufacturing networks are structured like those elsewhere, there is a greater risk of more widespread disruption from third-party threats. This is because of that IT-OT-IP convergence. Hackers could steal sensitive designs, highly regulated customer and employee personal data, or pivot from the IT into the OT network to sabotage factory processes.

Unfortunately, many manufacturing firms are falling at the first hurdle when it comes to cyber resilience. Regular patching remains highly problematic, in many cases because of long replacement cycles for hardware and software, allied to a mentality of 'do not touch' for operational equipment. This OT mindset, which prioritises uptime above cyber risk, can end up creating serious gaps for attackers to exploit. It remains difficult for many to reconcile the fact that heavy machinery may last 20-30 years, while computers and related equipment have an average lifetime of around nine years.

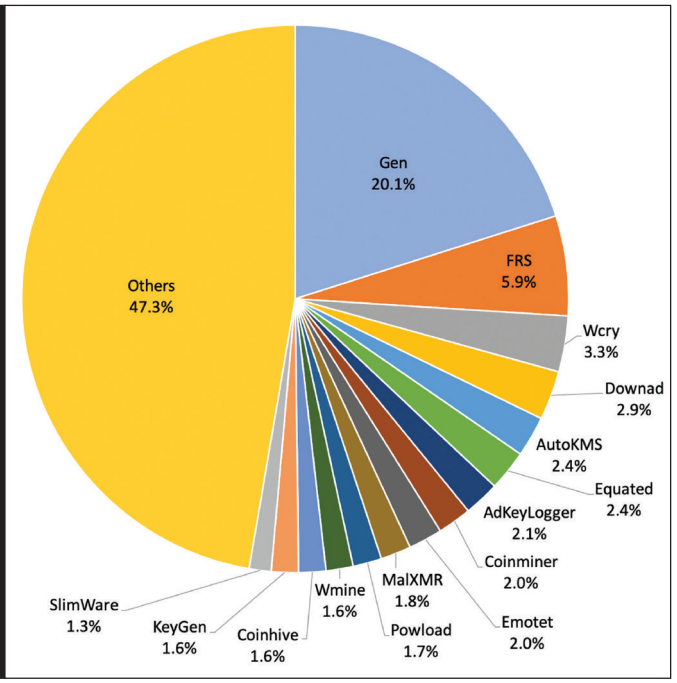
The result is hardware running seriously outdated software and operating systems. A scan run between July and December 2018 revealed only 29% of manufacturers had systems running Windows 10. The vast majority (60%) were still on Windows 7, while a significant minority (4.4%) had machines still running XP. The latter was almost double the number of organisations from other industries running XP (2.5%).

Perhaps unsurprisingly, Downad (aka Conficker), WannaCry and Gamarue (Andromeda) malware featured relatively frequently on machines used in manufacturing environments. Downad is over a decade old now, highlighting the patching challenge facing organisations in this sector. It also propagates commonly via infected USB sticks, by abusing autorun.inf. In fact, the manufacturing industry is more vulnerable to USB malware than any other industry, accounting for over a quarter (25.8%) of autorun.inf detections found by the research.

Cyber attacks might target data theft, look to extort victim organisations via ransomware or even generate profits from ille-




Operating systems in use by manufacturers. Source: Trend Micro.




Top malware families in the manufacturing industry. Source: Trend Micro.

gal crypto-currency mining. Ransomware in particular is becoming increasingly targeted in nature, and could have serious repercussions for the sector. The LockerGaga variant that infected Norwegian giant Norsk Hydro back in March 2019 cost the aluminium manufacturer nearly $52m in the first quarter alone.[3]

***"Whereas in the past they may have relied on 'security by obscurity' to stay safe from prying eyes, ubiquitous connectivity has rendered this approach largely ineffective"***

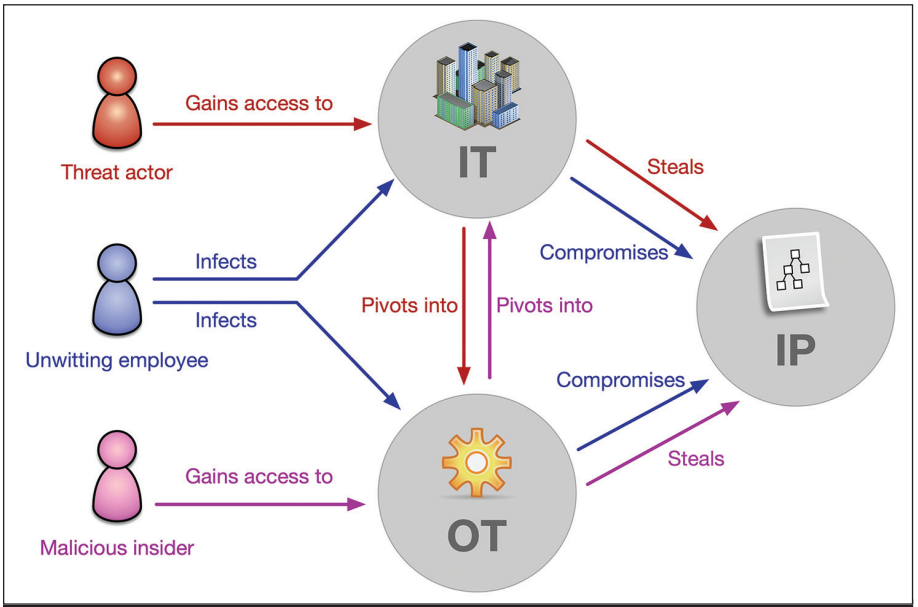
Increasingly sophisticated multi-stage ransomware attacks are being used to target manufacturing firms. In China, a campaign targeted vulnerable web services used by victim organisations to install the PlugX RAT usually associated with industrial espionage. This backdoor was used to maintain persistence, before a Mimikatz tool was uploaded to steal credentials and enable lateral movement. Finally, the attacker encrypted all files on the compromised machines, demanding 9.5 Bitcoins in payment (£65,134). Interestingly, the attackers had already downloaded crypto-mining malware on the compromised systems, in a bid to maximise their ROI.

## From cyber to physical danger

As IT and OT systems increasingly converge under the new banner of Industry 4.0, manufacturing organisations are becoming exposed to greater risks. Whereas in the past they may have relied on 'security by obscurity' to stay safe from prying eyes, ubiquitous connectivity has rendered this approach largely ineffective. That puts production lines, supply chains, and sales and enterprise systems at greater risk. There are several areas of concern, including vulnerabilities in industrial control systems (ICS), malware targeting these same systems and poor design or misconfiguration of networks.

The number of ICS bugs reported to the Zero Day Initiative in 2018 stood at 467, a massive 224% increase on the 2017 figures.[4] Over 60% of vulnerabilities were in human-machine interface (HMI) software for industrial control system (ICS) and supervisory control and data acquisition (SCADA) environments. Common issues included memory corruption (stack- and heap-based buffer overflows and out-of-bounds read/write vulnerabilities), poor credential management (use of hard-coded passwords, storing passwords in recoverable format, and insufficiently protected credentials), and lack of authentication and unsecure defaults (clear text transmission, missing encryption and unsafe ActiveX controls).

Sometimes it's not even necessary for attackers to exploit a vulnerability in such systems. HMIs have been exposed to the public-facing Internet without any authentication, potentially putting them at risk of remote control by attackers. In many cases you can find malware families designed to scan for ICS systems from the IT network, although thankfully thus far we've not seen malicious code designed to spread from HMI to HMI or from PLC to PLC. Service disruption, sabotage of key processes, extortion, production delays and even




How threats can figure into the IT, OT and IP convergence. Source: Trend Micro.

physical risks to manufacturing employees are all potential impacts.

## A trove of valuable IP

Yet it's not all about impacting physical manufacturing processes. Sometimes hackers are also after sensitive IP. The bad news for manufacturers is that it's not necessarily difficult to steal the kind of product designs, information on manufacturing processes or other sensitive data that could destroy their competitive advantage.

***"Lost IP of course not only impacts a manufacturer's competitive advantage, it can also drive a surge in counterfeit products. These now represent 3.3% of world trade"***

Malicious computer-aided design (CAD) documents are more common in this sector than any other, accounting for 23% of the total found by scans. For example, CAD malware ACM_MEDRE.AA looks for personal storage files in Outlook personal information manager and any other CAD files in a compromised machine and sends them to a predefined external email address. Bursted and Passdoc remain the most common CAD malware variants, despite being around since the early 2000s.

Other attacks may use malicious macros in Word documents, while unauthorised document sharing between departments, vendors and third parties can create additional security risks. Unintentional leaks may also occur due to poorly configured FTP servers. Lost IP of course not only impacts a manufacturer's competitive advantage, it can also drive a surge in counterfeit products. These now represent 3.3% of world trade, or $509bn, based on 2016 Customs seizure data.[5]

## Breaking down siloes

It goes without saying that there's a thriving dark web market in ICS/SCADA-specific hacking and password-cracking tools, as well as rising demand for CAD and computer-aided manufacturing (CAM) files, source code and other confidential documents. It's easy to predict that, as in other areas of cybercrime, the industrial espionage space will eventually become commoditised. While most of this is financially motivated activity, there are also drivers for nation state attackers to steal sensitive IP and sabotage facilities.

All of which begs perhaps the most important question: how do I improve my organisation's cyber resilience?

Fortunately, there are some basic, low-cost steps that can help, including restricting user access and permissions, and ensuring that file and web servers are restricted only to those who need to read, modify and or create files. Restrictions should also be extended to limit which corporate machines can talk to each other. This is especially important to segregate production machines from regular PCs on the corporate IT network, for example. Also any unnecessary networking services should be identified and removed to reduce the corporate attack surface.

***"Cyber security must be considered at the inception of any new IT or OT system design and/or purchase. This security-by-design approach is demanded by the GDPR and NIS Directive. But more important, it just makes business sense"***

These should by now be well understood best practice tips. But perhaps one of the most important things you can do is to encourage greater co-operation between IT and OT teams. As discussed, the former is usually more focused on data security while the latter prioritises safety and availability, which can create dangerous security gaps. Both need to shift their position in order to ensure that both IP and operational efficiency are protected from outside influence. Before you draw up a plan with shared goals, it's essential to understand and prioritise all the IT and OT assets in the organisation: everything that is connected to the IT network, plus any associate software, services and operating systems.

To combat the patching challenge, consider setting up isolated environments on which to test security updates. They can then be applied to production environments with more confidence that they won't break, crash or interfere with mission-critical systems. Virtual patching, intrusion detection systems (IDSs) and application control can provide a cheaper alternative with less risk of interfering in operations.

It should go without saying that end user education must be enhanced to enforce strict policies over data sharing and security. More broadly, cyber security must be considered at the inception of any new IT or OT system design and/or purchase. This security-by-design approach is demanded by the GDPR and NIS Directive. But more important, it just makes business sense to prioritise security when buying a new piece of technology that may last three decades. International standards like IEC 62443 can also help marshal efforts.

A quarter (24%) of UK manufacturers claimed last year to have suffered financial or other business losses stemming from a cyber attack, according to industry body Make UK.[6] Worryingly, 41% claimed they don't have access to enough information to assess their true risk exposure. The stakes are too high to ignore the cyberthreat. Visibility is the first step to improving control and mitigating risk.

### About the author

*Ian Heritage is a cyber security architect at Trend Micro UK, advising large companies on cyber risks and building resilience. He studied computer science at Oxford Brookes University and has worked at some of the industry's leading companies in technical advisory roles, including Sophos, ForcePoint (Raytheon) and most recently Trend Micro. Heritage is a speaker at industry events and is frequently interviewed by key technology publications.*

### References

1. 'UK Manufacturing Statistics'. The Manufacturer. Accessed Oct 2019.

www.themanufacturer.com/uk-manufacturing-statistics/.
2. Bakuei, M; Flores, R; Kropotov, V; Yarochkin, F. 'Securing Smart Factories'. Trend Micro. Accessed Oct 2019. https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf.
3. 'Norsk Hydro cyber attack cost it nearly $52m in first quarter'. Reuters/Insurance Journal, 30 Apr 2019. Accessed Oct 2019. www.insurancejournal.com/news/international/2019/04/30/525093.htm.
4. 'Caught in the net: unraveling the tangle of old and new threats'. Trend Micro. Accessed Oct 2019. https://documents.trendmicro.com/assets/rpt/rpt-unraveling-the-tangle-of-old-and-new-threats.pdf.
5. 'Trade in fake goods is now 3.3% of world trade and rising'. OECD, 18 Mar 2019. Accessed Oct 2019. www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm.
6. 'Cyber security for manufacturing'. Make UK. Accessed Oct 2019. www.makeuk.org/Insights/Reports/2019/02/11/Cyber security-for-Manufacturing.

# The state of operational technology security


Steve Mansfield-Devine

**Steve Mansfield-Devine, editor, *Network Security***

**It's a sad and worrying fact that awareness about cyber security – and subsequent action – has lagged behind as technology has progressed. This is true in every domain, but perhaps none more so than operational technology (OT). The systems used to run manufacturing plants, control power stations and water utilities and manage countless industrial processes – with many of the installations being deemed critical national infrastructure (CNI) because of their importance to safety, daily life and a country's economy – have often been left poorly protected from cyber attacks. In this interview, Tim Ennis and David Gray of NTT Security discuss the state of OT security and what can be done about it.**

It's not as if organisations haven't been warned. Over the past year or so, industrial firms have increasingly found themselves being targeted with ransomware, although such attacks tend to be against the business IT side of the operation. Back in 2015, malware known as Black Energy, capable of conducting espionage as well as sabotage operations, was found being deployed against industrial control system (ICS) installations in the US. Infamously, Ukraine suffered two major blackouts in cyber attacks on its power grids in 2015 and 2016.[1] And even more notorious was the 2010 Stuxnet attack against Iran's nuclear processing facility.[2]

These are just the high-profile incidents that garner headlines. Many organisations running OT find themselves the targets of continuous probing and attacks – at least, they do if they're paying attention. The concern, then, is whether they're ready to withstand serious attacks.

"OT security's still pretty much in its infancy," says Gray. "It's been about nine years since the attack in Iran, but vendors have only just, in the past couple of years, been coming to the marketplace with the tools that are able to identify and detect threats in an OT environment. It's starting to get a lot more traction now, with the likes of Clarity and Nozomi producing equipment that is able to detect threats and throw those up into the SIEM [security information and event management] space."

***"We didn't have to consider security because there was no perceived cyberthreat. A lot of it comes down to what has been the norm"***

He cautions, however, that the availability of tools has not been matched by an awareness at board level within OT organisations that they need them. Understanding of the security threat and how to respond to it is not at the same level as with IT operations in businesses in general.

The General Data Protection Regulation (GDPR) has done a lot to alert the C-suite to the need for information security in business networks, reckons Gray, and there's a possibility that the companion regulations aimed at the OT environment – the EU's Network and Information Security (NIS) directive – could have a similar effect on the industrial side of things.[3] But it's too soon to tell.

## Lagging behind

Why has OT security lagged so far behind IT security when it comes to awareness, solutions and action? Ennis believes we need to look at the history of the technology.

"Some of the OT systems I've worked on were operating way before any email systems were installed on site at power stations," he says. "We didn't have to consider security because there was no perceived cyberthreat. A lot of it comes down to what has been the norm."

The considerations given to the design and operation of OT systems were around efficiency, throughput, health and safety and regulatory compliance, he says. Even if an organisation had a senior

Tim Ennis is a senior operational technology consultant for NTT Security. In this capacity he is responsible for performing professional services engagement for operational technology (OT), including performing assessments, producing reports, and supporting security operations centre (SOC) design and delivery. Ennis has been working in the field of industrial control systems and OT since 2008. Previously having specialised in instrumentation and control (I&C) systems and safety instrumented systems (SIS) in the civil nuclear sector, he has since developed his OT security skills and knowledge to complement his engineering background. Ennis has experience of developing and implementing security programmes for ICS, including risk assessment methodologies, technology assessment and supply chain assurance. Prior to NTT Security, Ennis was a lead control and protection engineer in the civil nuclear sector, responsible for specification, design oversight and acceptance of high-integrity systems through to development, testing and commissioning of major projects. Additionally, he chaired civil nuclear sector information exchanges, represented utilities on government-sponsored cyber defence exercises and collaborated with nuclear utilities in the UK, US and Japan.

executive charged with security – a CISO, for instance – the OT side of the business would typically not fall within that person's remit. And this situation often persisted even as an increasing proportion of OT systems became networked and Internet-connected.

"That's starting to change," says Gray. "CISOs are starting to talk to their industrial counterparts and in some cases the CISO is becoming responsible for the OT infrastructure as well, or at least the network elements." This has been spurred on, over the past decade or so, by the accumulating list of incidents. As Gray points out, "OT organisations can no longer tell themselves they're not targets."

## Greenfield sites

Often, poor OT security is a legacy issue. Many of the components of an industrial installation might have lifespans measured in decades. Replacing something that still has a useful working life of 10 or 20 years just because the latest model can be more easily secured, isn't an option. But what about new factories, power stations or other installations?

"With a greenfield site, there is the opportunity to follow all the right design processes and apply the right architecture from day one," says Ennis. "That's not to say there aren't still some challenges, because often projects will follow a similar track to what's been done before. They might end up with a repeat of a previous project installation, with the same types of equipment. So you might still be using equipment that still has vulnerabilities. And it's more than just the technology piece. You still need the right processes and the right organisation to stay on top of it. Your first client modification might introduce risk into the system again."

The extent to which you can secure equipment depends in part on the vendors of that kit.

"Some of the vendors have been very good at listening to what organisations are asking for, and also leading, recognising that there's an issue and designing with security in mind," explains Gray.

There has been some progress in certifying equipment to show that it can meet certain security standards – although that still depends on the buyer installing and connecting it correctly. However, security is only one of the items on a buyer's wishlist and may be a low priority compared to the capabilities or available configurations of the equipment. And so while the equipment that meets the buyer's most important requirements might still have, say, Internet or file transfer capabilities, it is often still up to the buyer to secure them.

## Security through obscurity

Historically, OT organisations have often relied on a form of 'security through obscurity'. The protocols, data formats and interfaces used in OT systems are often complex and proprietary, and very different from those deployed in IT systems. It was difficult for an attacker to gain sufficient knowledge and expertise in those systems to mount a successful attack. But two things have changed that lift the veil on that obscurity – the Internet and the nature of the attacker.

Internet-based search tools such as Shodan make it relatively easy to find specific types of systems that are online. The web provides a wealth of shared information about such systems. And when it comes to mounting attacks on CNI organisations, the malicious attackers are, more often than not, well-resourced

David Gray is a senior manager for NTT Security. In this capacity he is responsible for managing professional services engagement for incident response across EMEA, security operations centre and computer incident response centre (SOC/CIRC) redesign, security gap analysis and roadmap services and other various security-related consulting engagements. Gray specialises in OT security engagements and has delivered SOC builds for major oil and gas and national power grid organisations. Prior to moving to NTT Security, he was an advisory consultant and engagement manager for a global security vendor where he delivered security consulting services around EMEA and APAC and as an incident response team leader for a major UK defence contractor where he investigated and co-ordinated all cyber security incidents across the company. Gray spent his formative years within the UK's Royal Air Force where he worked on most of the UK's secure communications network. He led the malware analysis team and was responsible for defending MOD network assets against computer network exploitation attacks from various APT groups.

groups, nation-state hackers who are prepared to invest heavily in their activities. This can mean spending a lot of time on reconnaissance and footprinting targets or it can mean replicating industrial systems in order to explore their weak points.

"When you're talking about nation-state attacks, these are countries that can afford to purchase an entire OT infrastructure to be able to take it to pieces, to understand how the protocols work," says Gray.

However, it would be a mistake to view attacks on OT systems, even CNI organisations, as being purely about some kind of undeclared cyberwar. The impact of regular, run-of-the-mill cyber criminals can't be ignored, and is even increasing. Hackers have identified the industrial sector as one where downtime is expensive and hard to tolerate, and which is therefore ripe for exploitation via ransomware.

This fact was dramatically demonstrated in the attack on Norsk Hydro in March 2019.[4,5] The firm's response was textbook: it refused to pay up and reverted to manual systems to cope with the interruption. Nonetheless, at the last count the incident was calculated to have cost the company $75m.[6] How much of that loss is insured is unclear. What is certain is that the attack demonstrates how even meagrely resourced attackers can cause major disruption.

## Self-awareness

Given the rising concern over the threat to critical infrastructure and the increasing number of attacks on OT networks, you would assume that organisations operating in this area would be fully aware of the dangers. There is a slight problem, however, that the focus has shifted too much to OT.

"When people look at the OT threat, they're still thinking of the grander scale, about Dark Energy, Stuxnet, that sort of thing," says Gray. "I don't think everybody has cottoned on yet to the fact that the more commodity type of malware is still applicable to their networks, at least to the more traditional sort of Windows-type boxes that support higher layers within their OT infrastructure."

This isn't helped by the ever-greater convergence between IT and OT. This has been going on for some time, and there's a danger that organisations fail to get an overall picture of the attack surface.

"It's whether organisations have full visibility of what their connections to the Internet are," says Ennis. "It's not just about your direct connection to the Internet; it's how the rest of the network is put together and how it's operated – if you have connections in for the supply chain, or you have vendor support coming out on site with their own laptops or USB sticks."

***"It's not just about your direct connection to the Internet; it's how the rest of the network is put together and how it's operated"***

Achieving a full understanding of where you stand requires a consolidated approach, encompassing both IT and OT.

"The two need to be considered together," adds Ennis, "because ultimately if you have an OT network that's doing something – producing electricity or water, say – then the enterprise network is there to support that operation."

## Assessing risk

Organisations can get help with assessing risk through the use of tools and frameworks, much as with conventional business IT. They may have more of a challenge adapting their processes if these were established before the Internet changed the nature of their networks.

"Deciding which methodology they should choose to best fit within their existing processes can be difficult," says Ennis, "because it's much more challenging to tack a cyber risk assessment and a cyber set of controls onto an existing design and process. Ideally what you want to be able to do is combine the two so that you can get the best outcomes from assessing and applying the right controls at the right place, to complement your design rather than trying to add on security controls at the end."

It's not as though security is something you do once, either. Most organisations in every sphere have trouble staying current with the threats they face. But if you're installing systems that are going to be in use for 30 years, then ensuring they remain resilient to rapidly shifting cyberthreats is that much more of a challenge. But there are signs that organisations are engaging with this problem, says Gray.

"It's something that has changed just in the last year or two," he explains. "A lot of OT environments tended to be very flat networks. There was no segregation. If an attacker was able to get inside, he could navigate and do pretty much anything he wanted. But organisations are starting to segregate their OT environments into different sections for different vendors, so that you're splitting up your OT environment a little bit, to give you more security."

***"What the standards do is put organisations in the best possible place, to have resilient architectures and processes, so you aren't then, on a daily basis, trying to keep up to date with the latest threat"***

There are now some useful guidelines, most notably from the US National Institute of Standards and Technology (NIST).[7] But even these have trouble keeping up with the times.

"It is a big challenge," says Ennis. "When a standard is developed, it takes quite a long time to have it ratified and reviewed and published, and then also it has to be adopted and assessed again. But what the standards do is put organisations in the best possible place, to have resilient architectures and processes, so you aren't then, on a daily basis, trying to keep up to date with the latest threat and having to react to it. You need to be proactive. Following the standards gives you a good position to start from and then you have to understand what your assets are, what equipment you have, where it is, how it is configured and what it does."

That's not always simple, though. Many organisations above a certain size struggle with knowing exactly what exists within their IT estates. The same goes for OT.

"You can't protect what you can't see and can't identify, so the identification piece is absolutely key," says Ennis. "One of the big challenges is, how do we get this visibility into our OT networks? We might have a good understanding of what types of systems we have, but maybe not actually how they are connected and how they're communicating. One of the trends that's been fantastic to see over the past few years is the technology that's out there now to help organisations understand not just the assets that they have, but how they're connected and even the levels of patching and the status of those devices on the network. This could really help them understand if there is a risk here. And what actions they need to prioritise to reduce that risk."

## Particular spin

Other aspects of OT security have parallels with IT, although sometimes with a particular spin. Patching presents similar problems and has similar solutions, although organisations running critical systems, such as electricity distribution, might have to have stronger motivations to take important systems offline in order to patch them.

"The pinch point still comes down to an organisation knowing which patch to apply and when," says Ennis, "and how to make sure that that patch isn't going to cause them any disturbances in their installation of that equipment."

Gray adds: "One of the other points that organisations have to look at is that patching isn't the be all and end all. If there is a threat, it's understanding what the threat is, and then mitigating that on the system – whether that is something as simple as locking down the firewall between devices. It's about identifying how to be able to stop the attack before it gets onto the vulnerable system in the first place."

As in all sectors, there's a trend towards using anomaly detection, active monitoring and feeding data into SIEM systems in an attempt to improve situational awareness.

***"If we have all these logs and all this monitoring for our OT equipment, how do we know that we're actually looking for, monitoring and alerting off the right incidents?"***

"There's still the challenge of how that's applied to legacy networks," says Ennis. "You need to get that understanding of what you're actually looking for. If we have all these logs and all this monitoring for our OT equipment, how do we know that we're actually looking for, monitoring and alerting off the right incidents? So it's a challenge to get that development or that installation of the equipment in the right way, and get it set up to fit into the organisational context. Do you have the resources to be able to look at these logs? And what do you do if you do find something? What's the response mechanism? Do you have field engineers, or does it come from some central SOC? That's the challenge."

## Incident response

One area where things can be very different concerns incident response.

"From the OT perspective, we're not looking at the traditional IT CIA [confidentiality, integrity, availability] triangle," says Gray. "We're looking more at the risk to life for human beings themselves from cyberthreats, and to the overall production environment – what happens when your power station goes down and a couple of cities lose their lights. So, from the response side of things, it tends to be more of an impact than it would be with your traditional IT space."

There may be aspects of the OT environment that throw up additional issues when it comes to response. There are more factors to consider because this isn't purely an IT environment – it's an engineering and production one too.

"Whether it's IT or operational technology, we always recommend that organisations build an incident response plan, so that they understand what they are going to do before something happens," says Gray. "And within the OT environment that's especially relevant because every system's different. Organisations have to be able to understand what the impact is of a system going down."

It's hard to say what proportion of organisations have that maturity, with detailed plans in place. But as Ennis points out: "With the NIST regulations now, any organisation that is deemed an operator of an essential service will have to demonstrate their capability and show that they have these response plans, as well as having their response plans tested."

## Cost issue

NIST regulations apply specifically to CNI organisations. There are, of course, plenty of firms running OT environments that don't fall into the category of critical infrastructure. Whether they will go along the same path as those organisations pushed down it by the NIST regulations remains to be seen.

"It is always going to be a cost issue, and it could be that some organisations will react and put these plans in place when they have an incident themselves and realise the importance of having the plan in place," says Ennis. "If we look what happened with Norsk Hydro and their response to the incident, they obviously have invested in having that capability. Organisations that are not CNI and don't fall under the NIST regulations might not be incentivised in the same way to have these security programmes in place, but I think there will be enough headline stories that organisations will understand they have to do something. They have to work out what is the most proportionate security that they need for their operations. And having a security plan in place that allows them to test their response to incidents should be seen as an absolute must if they want to continue doing what they do."

## The future

Those headlines Ennis referred to are becoming more frequent and it would be easy to develop a sense of doom, especially as nation states increasingly flex their cyber

muscles. So are Ennis and Gray optimistic or pessimistic about the future?

"I am quite optimistic," says Gray. "There are challenges coming in the future with the likes of 5G. But the fact that there's a lot more awareness of the problem is helping drive the solutions. And there are vendors from the network security side of things that are starting to realise that they have the opportunity not only to make money themselves, but to be able to help defend these networks."

Ennis agrees: "We have to be positive. There is fear, uncertainty and doubt around this subject, and it's been there for long enough that there has been sufficient discussion in organisations. And regulation is really making a difference. There is some scary stuff out there, but it's not about trying to make things perfect overnight, it's about understanding where you are now, what you're trying to aim for, and then working towards it, and if that means that you have to do a high-level assessment to begin with, and implement some interim controls, then so be it, but at least you are on the road to improving, and that can only be a good thing."

## About the author

*Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security and its sister publication Computer Fraud & Security.*

## References


1. Zetter, Kim. 'The Ukrainian power grid was hacked again'. Vice, 10 Jan 2017. Accessed Oct 2019. www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.
2. 'Stuxnet'. WIkipedia. Accessed Oct 2019. https://en.wikipedia.org/wiki/Stuxnet.
3. 'NIS Directive'. ENISA. Accessed Oct 2019. www.enisa.europa.eu/topics/nis-directive.
4. Fiveash, Kelly. 'The Norsk Hydro cyber attack is about money, not war'. Wired, 21 Mar 2019. Accessed Oct 2019. www.wired.co.uk/article/norsk-hydro-cyber attack
5. 'Cyber attack on Hydro'. Norsk Hydro. Accessed Oct 2019. www.hydro.com/en/media/on-the-agenda/cyber attack/.
6. Ashford, Warwick. 'Norsk Hydro cyber attack could cost up to $75m'. Computer Weekly, 23 Jul 2019. Accessed Oct 2019. www.computerweekly.com/news/252467199/Norsk-Hydro-cyber attack-could-cost-up-to-75m
7. 'Cyber security framework'. NIST. Accessed Oct 2019. www.nist.gov/cyberframework.


# Cyber security attacks on robotic platforms

**Dr Akashdeep Bhardwaj, Dr Vinay Avasthi, University of Petroleum & Energy Studies, India; Dr Sam Goundar, University of South Pacific, Fiji**

Dr Akashdeep Bhardwaj

Dr Vinay Avasthi

Dr Sam Goundar

**Robotic technology has been rapidly transforming world economies in terms of business productivity and profitability. The market is shifting towards optimisation and automation – not just for the warehousing and manufacturing sectors, but even non-industrial areas such as defence, farming, hospitals, offices and even schools. The availability of open source platforms, falling hardware and electronics prices, prompt prototyping and convergence of technologies are some of the major reasons for this new revolution. However, cyber security and physical threats are high-priority areas when critical applications and missions are involved.**

The term robot is technically defined as a non-human component designed to perform automated tasks with speed, precision and efficiency, in a repeated manner. From an industry standpoint, robotics involves three critical business roles.

First, there's automation, which executes applications in the form of software robots. These in turn control, deploy and – for business applications, which involve multiple systems – automate tasks normally performed manually. Such activities may involve direct interactions with a user interface. No software code is written to automate individual tasks as the software robots are trained to assist human staff. This includes data manipulation and migration across various systems and rule-based decision-making.

Second, there's orchestration which focuses on automating time-intensive tasks and streamlines complex workflows on operational activities such as IT service management, incident response or provisioning and de-provisioning users. This involves significant software development efforts to set up predefined workflow rules, which take business decisions and involve the use of application programming interfaces and database servers.

| Business Attribute | Automation | Orchestration | Cognitive Learning |
|---|---|---|---|
| Trained by business experts | Yes | No | No |
| Interacts with user interface | Yes | No | No |
| Intelligent, self-controlled | Yes | No | No |
| Decision-making based on defined rules | Yes | Yes | No |
| Train IT admin/security team | No | Yes | No |
| API interactions with back-end database | No | Yes | Yes |
| Requires efforts for code development | No | Yes | Yes |
| Involves developers and programmers | No | No | Yes |
| Uses AI, ML, analytics | No | No | Yes |

**Table 1: Key attributes involved in robotic systems.**

Finally, cognitive learning involves the use of analytics and advanced algorithms, and incorporates machine learning and artificial intelligence similar to humans. This, however, requires the modelling of self-learning and machine algorithms and extensive programming. These aspects attributed to robotic systems are shown in Table 1.

Robots are commanded and controlled by humans or applications. They are classified as autonomous, insect or androids. Autonomous robots do not need to be guided by manual intervention and have the ability to carry out commands. Insect robots perform functions on the basis of single command controllers like a colony of insects following a single leader. Androids are intelligent robots using machine learning and artificial intelligence to learn and respond to situations and tasks assigned to them.

***"The lack of security governance standards and vulnerability assessments for robotic systems makes them vulnerable – more so when connected to cloud-based Internet of Things (IoT) networks"***

Robotics uses application software, control systems, sensors and networks for communication and effective control. However, the lack of security governance standards and vulnerability assessments for robotic systems makes them vulnerable – more so when connected to cloud-based Internet of Things (IoT) networks, which can expose robots to potential cyber attacks, or the use of collaborative systems and sensor nodes that send commands and data over Internet networks.

## Literature survey

The authors analysed research papers from the past few years focusing on cyber and physical security attacks on robotic systems and which involved robots, IoT sensors and networks.

Al-shukri et al proposed the use of a thermal imaging camera and robotic systems to detect infiltrators and intruders in border defence systems.[1] These systems involved the integration of network links that shared images to the command centre with robotic motors connecting infrared and laser guns and IoT sensors for sound detections. Decisions were performed for initiating detection and mitigation processes.

Tanjim et al reviewed several theories on resolving traffic jams in cities and presented a robotic flight control system for vehicular movement, which potentially resolved roadblocks and traffic jams.[2] The system co-ordinated vehicles for their turns and forward and backward moves.

Uddin et al presented a prototype for controlling remote unmanned aerial vehicles.[3] This model provided help in security monitoring and the cleaning of high-rise buildings for maintenance. The device was built using a frame, motors, speed controllers, development boards and sensors. Battery, transmitter, receiver and GPS were interfaced with Internet connectivity. This was a collaborative platform that faced cyber and physical risks after implementation.

Haus et al presented experimental results on aerial and underwater robotic vehicle control.[4] The authors used a centroid vector algorithm for dynamic and static control of actuators. This assisted in controlling the orientation of the robot parts, payload and sensors. The simulations were replicated on different platforms, which displayed that the experiment could be translated across various robotic platforms for different industries.

Zhang et al designed a secure, effective access control model for emotion analysis for interactive robots.[5] This model utilises machine learning and cloud-based access for providing emotional care to users. Privacy, authentication and authorisation issues were addressed using a polynomial cloud-based security policy. The model was implemented and verified in a test bed environment on a robotic platform.

Lakki et al (2019) developed a prototype to address cyber security challenges for IoT and future devices, such as the use of mobiles for remote surgery using robots.[6] This involved the design and implementation of a digital twin model that takes the input of all data sources and communicates via a single interface. The authors concluded that such system would require multiple collaborations across various engineering domains. Since each industry uses different tools and processes, integrating each may not work well for mission-critical robotic systems and it would open up cyber security threats as well.

Liu et al focused on vulnerabilities of Google Play Store applications for robots.[7] The authors determined that the mobile to device network communication was unencrypted. This indicated that data transfer and commands are vulnerable to sniffing and man-in-the-middle attacks. The Android mobiles had privilege escalation issues. Using

experimental attacks, the authors presented a proof of concept to provide solutions to mitigate these threats.

Farris et al presented an analysis of cyber security attacks on IoT and robotic platforms and the vulnerabilities faced by software defined networks and virtualisation technologies.[8] The authors also discussed the challenges of – and presented mitigation approaches for – IoT solutions, and compared them with traditional countermeasures.

***"Mechanical parts inside robots – such as grippers, motors, gears, wheels or pistons – that enable robots to move, grab and lift items, pose serious threats if controlled by malicious attackers"***

Hasan et al designed a robot prototype that combined remote access and control using ultrasonic sensors for enhanced security.[9] The model also performed the role of sending intruder images over networks for indoor environment security and for obstacle avoidance and real-time movements. They presented the results and secure coding details.

Basan et al analysed the impact of denial of service attacks on mobile robotic nodes.[10,11] The authors presented suitable parameters for detecting DoS attacks and developed a methodology for the security verification of robots.

Okuri et al designed an algorithm for network-based transmission to detect and block eavesdropping on wireless sensor nodes.[12]

Lambert el al proposed bridging the gap between safety and security for real-time, intrusion-tolerant systems in relation to cyber and physical attacks against the latest threat vectors.[13]

Guo et al proposed using blockchains for recording accidents and attacks involving autonomous vehicles.[14] The system sent logs as proof-of-events to a blockchain for thorough, trusted and verifiable forensics investigation. This involved no central monitoring and recording authority.

Sentsov et al presented security issues on wireless communication links between a control panel system and an unmanned vehicle.[15] Protections against unauthorised external attacks and mitigation solutions for interception of controls were presented.

Stevano Zanero discussed the security challenges for digital components involving cyber systems and physical components.[16] The author analysed key case studies on sensors and network integration.

## Cyberthreats

Cyber security and physical attacks on industrial and production robots result in massive risks to life and property. Mechanical parts inside robots – such as grippers, motors, gears, wheels or pistons – that enable robots to move, grab and lift items, pose serious threats if controlled by malicious attackers. Communication network links between humans and robotic platforms face severe cyber security threats from hacks. These include the use of insecure protocols and system configurations, malware, man-in-the-middle and denial of service (DoS) attacks. Reasons for the vulnerabilities and subsequent cyber security problems in robots include:

- Lack of secure networking between the command centre and robot.
- Authentication issues leading to unauthorised access (using standard username and password).
- Lack of encryption, which exposes sensitive data and design plans.
- Misconfiguration of robotic systems – hardware features and programs.
- Lack of proper physical access controls inside robotic labs and assembly centres.

Some of the recent incidents associated with cyber and physical attacks involving robots are detailed in Table 2.

Robotics systems function using computer hardware, operating systems and applications. Robotic setups are composed of hardware components such as sensors, adapters, LCDs, network cables, data communication and storage devices and software applications. Security threats are similar for both environments. In most cases, attacks on robotic systems involve attackers who have physical and logical access, are technically familiar with the robotic systems and have the skills to manipulate the robotic systems. Threat agents that can cause attacks in physical as well as cyber mode are detailed in Table 3.

## Research performed

The authors performed security vulnerability analysis of programmable robotic

| Timeline | Location | Event | Investigations revealed |
|---|---|---|---|
| May 2015 | Car factory, Cincinnati, US | Worker died due to skull crushed by robotic system that restarted unexpectedly | Malware on robotic platform corrupted the command sequence to load trailer on assembly robots. |
| August 2015 | Maruti factory, Manesar, India | Assembly line robotic arm grabbed a worker, who died | Industrial robot's cables tampered with; no security process followed. |
| April 2016 | US military base | Nine US soldiers shot dead by robot mortar gun in a training exercise | Robotic system malfunctioned due to malware in system. |
| December 2017 | Shopping mall, Silicon Valley, US | Toddler run over by robot used for cleaning floors | Robotic platform misconfiguration due to security flaw exploited by script kiddies. |
| March 2018 | Cambridge, UK | Robot thought 3D turtle was a rifle and attacked | Researchers altered a 3D image of a turtle to fool robotic AI and sensors. |
| June 2018 | Kyushu University, Japan | Changed pixels in photos to fool robotic systems | Robotic system using AI mistook cats for dogs, airplanes for dogs and even frogs for trucks. |

**Table 2: List of cyber security & physical security attacks by robotic platforms.**

| Threat agents | Motivation | Objective |
|---|---|---|
| Company insider | Disgruntled staff seeking revenge | Damage and halt production delivery |
| Competitors | Industrial espionage | Harm company reputation, business advantage |
| Wannabes | Fun, challenge or showing off to friends | Showcase newly learned skills |
| Malware | Seeking financial gain by employing ransomware | Deploy malicious payload seeking ransom |
| Cyber criminals | Display advanced capability | Target organisation or executives for blackmail |
| Missing security patches | Steal sensitive data | Gain remote, unauthorised access |
| Thieves | Seek ransom, business competition | Resell robotic parts, steal intellectual property |
| Nation states | Political gain or sway population groups via social networking | Destabilise organisation or country |
| Insecure configuration | Gain access, display proficiency for system on the Internet | Collaborative Industrial IoT from Internet |

**Table 3: Cyber security and physical threat agents.**

systems written in Python and Java. The code itself is confidential and not publicly available. The control logic module files were: Module-SupController.py for interactions between the robotic device and signals sent to the application for triggers and alerts around the desired behaviour; and Module-SupStateMachine.py representing the various states in which the sensors interpret robotic movements in the environment. Other modules involved in the platform were Sensor_Proximity, Wheel_Drive and Wheel_Encoder. Penetration testing of the robotic platform application was performed using specialised tools as well as custom, manual penetration testing. Tools used included:

- Echomirage: An open source tool that hooks into client executables and associated processes. It intercepts traffic between client and app platform logs and during validation of user ID and password.
- Process Explorer: This identifies files accessed or registry entries modified when the client executes the Python modules. Process ID (PID) executed on the client is vulnerable to malware attacks, turning the client system into a bot capable of controlling the robotic platform.
- Registry Editor (Regedit) displays the Windows Client Registry in a graphical manner, illustrating the entries and changes made by attackers. The authors established this by having a malicious payload disable the anti-malware and anti-virus programs on the client system as well as reading passwords.

## Summary of findings

The following are the top seven security issues discovered during the research.

**Rob-PL-001 –** Vulnerability type: information leakage. Threat priority: high. The authors found that use of a temporary App-ID is able to inject arbitrary and malicious code on the administrator system (Robo_Svr01) in script Chk-for-Update.py on line 425. The module scripts are vulnerable to an arbitrary code execution issue.

Recommendation: Strict input validation implemented in script (Chk-for-Update.py).

**Rob-PL-002 –** Vulnerability type: code execution. Threat priority: high. Input commands for the robot are allowed from untrusted sources excluding system administrator platform machines for command modules to move the robotic system (like move forward, roll backwards, move right or move left). With no IP restriction, untrusted clients on the robotic platform network can inject code that can affect commands for the robotic system. While there is a Bleach Sanitisation module check in use by the module (Com_In), the authors observed that this is possible to evade, as demonstrated with the following JavaScript insertion:

```
<a href="Javas&#127;Java-
script:alert(1)">Alert</a>
<a href="&#148;Java-
script:alert(1)">Alert</a>
```

Recommendation: IP whitelisting for systems running administrator activities should be limited to a maximum of two machines only – one acts as the primary admin system and the other acts as the back-up admin system; browser-based JavaScript to display the descriptions of package modules; use of the latest Bleach Sanitisation version 3.1.0 as of 9 January 2019.

**Rob-PL-003** – Vulnerability type: code execution. Threat priority: high. A malicious user can inject code in the administrator system (Robo_Svr01) in the build module (Build.py) on line 1043. This module can be made to accept the App ID as a parameter. Then the input is passed to the sub process shell as:

```
Sub-Proc-call("Rob-Srv02: Publish
{0}".format(App-ID))
```

Recommendation: The authors strongly advise that input requires validation before any input parameter can be accepted, such as in the case of App-ID.

**Rob-PL-004** – Vulnerability type: denial of service (DoS) attack. Threat priority: high. The use of predictable filenames in /tmp means that this insecure usage of temporary files can allow an attacker to perform a DoS attack that links to an important file module and overwrites critical files – for example:

```
dr-zer.console = p-expect_spawn
("dr-zer connect console")
dr-zer.logfiles = p-open
("/tmp/dr-zer_report.log", "w")
```

Recommendation: any export files generated should always be stored in a dedicated folder with limited, restricted user access permissions.

**Rob-PL-005** – Vulnerability type: arbitrary file download. Threat priority: moderate. The authors discovered that the robotic platform admin module does not validate the hash, size and type of files downloaded on mobile client systems via Bluetooth or wireless. This

can lead to the compromise of the client system when an insecure malicious APK file is injected.

Recommendation: All download activities, including transmission of data should be limited; only whitelisted file types should be allowed; this can be fixed by performing content type checks in the parent classes and subclasses.

***"Cyber criminals can easily exploit the robotic systems setup to gain access into the organisation's network and systems. Once inside, modifying, stealing or even destroying sensitive high-value data and accessing unauthorised applications becomes easy"***

**Rob-PL-006** – Vulnerability type: unverified trust issue. Threat priority: high. The robotic platform application logic is based on trust on first use (TOFU) using a non-verified certificate signing module function. As per the designers, this feature is a client demand.

Recommendation: A one-time password, PIN or fingerprinting mechanism should be implanted before any file exchange or download is initiated. While this cannot completely mitigate file-level attacks, potential device compromise can be minimised to a certain extent.

**Rob-PL-007** – Vulnerability type: insecure communication. Threat priority: high. In the file net/bluetooth/BluetoothClient.java, a Bluetooth device creates an insecure RFComm socket. This type of connection is vulnerable to man in the middle attacks, as the line key is not encrypted.

Recommendation: The integrity of communication is compromised, leading to arbitrary app installation and device compromise. An out-of-band key-sharing mechanism, such as sharing a password-protected file over an insecure RFComm socket, containing a symmetric encryption key, can be used to exchange keys between untrusted devices, instead of TOFU.

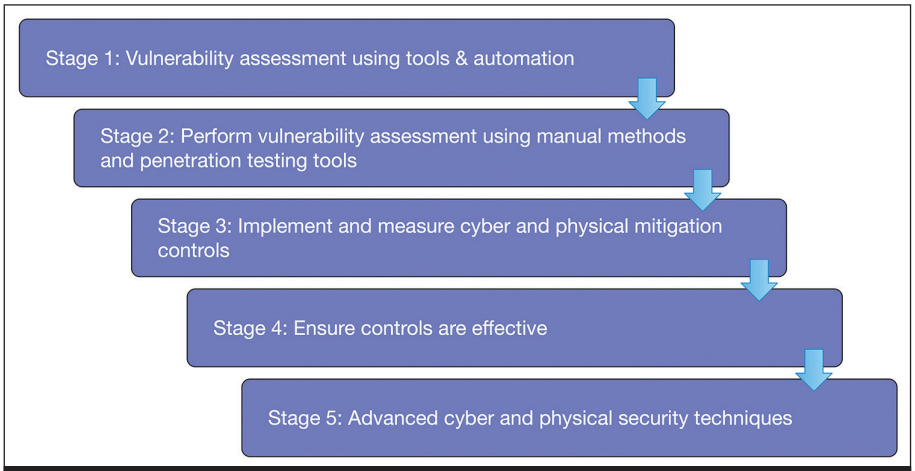



**Figure 1: Multi-stage approach for cyber and physical security.**

## Proposed CIA model

As collaborative platforms, IoT and Internet access converge for robotic implementations and new attack surface areas with previously unknown vulnerabilities have been uncovered. Cyber criminals can easily exploit the robotic systems setup to gain access into the organisation's network and systems. Once inside, modifying, stealing or even destroying sensitive high-value data and accessing unauthorised applications becomes easy.

***"The issue here is sensitive information and robotic systems being accessed or stolen by unauthorised threat agents. This involves loss of intellectual property, design, program code and system breaches"***

In order to address the core goals of security, the authors mapped the classic confidentiality, integrity and availability (CIA) triad model to address loopholes inherent in traditional security approaches for improving the cyber resilience of robotic systems.

**Availability**: This focuses on recovery from denial of service affecting communication channel bandwidth, application and systems resources and physical outage attacks on robots and platforms. Traditional processes involve determining the recovery objective, time lost with recovery point (maximum data lost) and then trying to recover the systems within the defined threshold times. This approach assumes recovery starts immediately after the disruption due to a TCP SYN flood attack, loss of connectivity or a man in the middle attack. Any breach needs to be investigated for loopholes and fatal flaws before recovery efforts are initiated, which can involve manual or temporary workarounds to restore the robotic system even as the platform recovery is being performed.

The proposed solution is to use automation, flexible processes and to empower the project team to use its resourcefulness and skills for effective decision-making instead of relying on scripted recovery actions.

**Integrity**: This is about manipulating data and traffic from clients to the robots, including applications and code. Robotic back-ups are primarily designed to protect against physical outbreaks, which involve hijacking the robot, or assault on physical equipment or the staff. This is accomplished by manipulating safety protocols, making the operators and machine vulnerable to destructive movements. Ransomware and attacks such as WannaCry impact system reliability, data and operations. The manipulation involves intercepting packets and replacing IP and checksums or encrypting the data on the controller. At times, as well as the production environment, the back-ups are also corrupted.

The proposed solution is to have off-network servers and platforms that run core services for testing and deployment, so that attacks can be avoided.

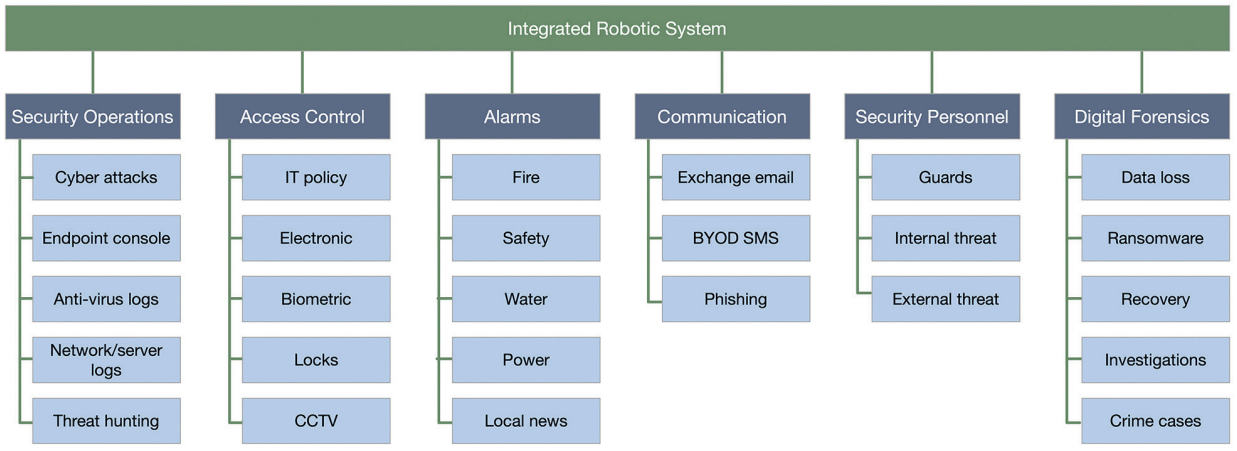



**Figure 2: Integrated cyber and physical security systems.**

These environments are air-gapped from external access. They do not connect directly to internal or external networks.

**Confidentiality**: The issue here is sensitive information and robotic systems being accessed or stolen by unauthorised threat agents. This involves loss of intellectual property, design, program code and system breaches. Current recovery practices normally do not involve any process for gracefully shutting down the breached robotic environments. Stop-gap alternatives to robotic processes are hurriedly implemented and service delivery and business is impacted until the investigations are completed.

The proposed solution involves designing an automated process that explores potential threats and proposes remediation activities before gracefully shutting down the critical services.

Cyber and physical security for robotic systems needs to implement a multi-stage approach, as illustrated in Figure 1.

## Mitigating attacks

Corporate enterprise and security centre teams are challenged by the use of multiple devices and applications generating different logs, utilising legacy technologies and in integrating all of these systems. The aim is to have a centralised, single pane of glass for cyber security and physical security control systems, integrated with the robotic system.

Typically in an organisation, the primary system includes security operations that involve the monitoring and detection of cyber attacks on assets, endpoint console management, analysing logs from anti-virus, networks and servers as well as use cases from threat hunting findings. The second system concerns the IT process, policies implemented for access controls with electronic, biometric, CCTV and physical locks. Alerts for fire, safety, water, power and local news should also be integrated as alarms. Inbound and outbound traffic information concerning emails, SMS and potential phishing traffic should be scanned on the integrated robotic system, as should security personnel-related reports by guards regarding external and internal threats. Digital forensics data regarding any data loss protection (DLP), ransomware recovery, ongoing investigations and criminal cases are sent to the centralised robotic system that integrates all the systems in this organisation. This is illustrated in Figure 2.

However, during the integration as illustrated in Figure 2, the physical and cyber security systems do not work well with one another. The fallback is to perform manual data gathering and application fine tuning of multiple systems, migrating information logs and databases from multiple systems or simply switching between multiple applications to complete the tasks. In order to resolve such issues and manage operating costs, organisations are using robotics to solve such issues – for example, to:

- Minimise incident detection and response time and requirements.
- Perform threat surface exposure checks against attacks.
- Automate repetitive and resource-intensive tasks.
- Minimise employee attrition due to lack of challenging work or career progression.
- Allow employees to focus on high-value and enhancement tasks.
- Perform automatic vulnerability scanning.
- Deploy cyber security and physical controls on potential risks.

## Conclusion

Delivery tasks in industry domains such as manufacturing, agriculture, logistics, healthcare, transportation, cyber and physical security are increasingly becoming dependent on robotic processes. Traditional access control systems cannot detect the recent vulnerabilities or defend against the latest, ever-evolving cyber security and physical attacks on robotic system availability, integrity and confidentiality. These issues impact not just the robots but are present at every level of hardware, networking, applications and platforms. It has become the responsibility of each individual involved in robotics to detect and mitigate the risks. For any robotic platforms and systems to be safe, the robots must also be cyber-safe.

### About the authors

*Dr Akashdeep Bhardwaj is currently professor of cyber security and digital forensics at the University of Petroleum and Energy Studies (UPES), Dehradun, India. He has over 25 years of IT industry experience*

*working for various US and UK organisations in cyber security, information security, datacentre operations, enterprise risk and resilience.*

*Dr Vinay Avasthi is an associate professor at the School of Computer Science, UPES and has 20 years of experience in research and teaching computer science. He is a life member of the Computer Society of India (CSI) and the Indian Science Congress. He is also a fellow of IETE India. His areas of interest are cloud security, software reusability, data science and cyber security.*

*Dr Sam Goundar has been teaching information systems, information technology, management information systems and computer science over the past 25 years at several universities in a number of countries at all levels. He is a senior member of the IEEE, a member of ACS, a member of the IITP, New Zealand, a certification administrator of ETA-I, USA and past president of the South Pacific Computer Society. He also serves on the IEEE Technical Committee for the Internet of Things, cloud communication and networking, big data, green ICT, cyber security, business informatics and systems, learning technology and smart cities. He is a member of the IEEE Technical Society and a panellist with the IEEE Spectrum for Emerging Technologies.*

## References


1. Al-shukri, D; Lavanya, V; Sumesh, P; Krishnan, P. 'Intelligent border security intrusion detection using IoT and embedded systems'. 4th IEEE MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, Feb 2019.
2. Tanjim, M; Oishi, A; Nandy, A; Jannah, R; Ahmed, S. 'A flight control system for a vehicle'. IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019.
3. Uddin, S; Hossain, R; Rabbi, S; Hasan, A; Zishan, R. 'Unmanned aerial vehicle for cleaning the high rise buildings'. IEEE International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019.
4. Haus, T; Orsag, M; Nunez, P; Bogdan, S; Lofaro, D. 'Centroid vectoring for attitude control of floating base robots: from maritime to aerial applications'. IEEE Access, Vol.7, pp.16021-16031, 2019.
5. Zhang, U; Qian, Y; Wu, D; Hossain, S; Ghoneim, A; Chen, M. 'Emotion-aware multimedia systems security'. IEEE Transactions on Multimedia, Vol.21, Issue 3, pp.617-624, 2019.
6. Laaki, H; Miche, Y; Tammi, K. 'Prototyping a digital twin for real time remote control over mobile networks: application of remote surgery'. IEEE Access, Vol.7, pp.20325-20336, 2019.
7. Liu, K; Shen, W; Cheng, Y; Cai, L; Li, Q; Zhou, Q; Niu, Z. 'Security analysis of mobile device-to-device network applications'. IEEE Internet of Things Journal, Early Access, 2018.
8. Farris, I; Taleb, T; Khettab, Y; Song, J. 'A survey on emerging SDN and NFV security mechanisms for IoT systems'. IEEE Communications Surveys & Tutorials, Vol.21, Issue 1, pp.812-837, 2019.
9. Hasan, R; Hussain, A; Nizamuddin, A; Mahmood, A. 'An autonomous robot for intelligent security systems'. 9th IEEE Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2018.
10. Basan, E; Medvedev, M; Teterevyatnikov, S. 'Analysis of the impact of denial of service attacks on the group of robots'. International IEEE Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Zhengzhou, China, 2018.
11. Basan, E; Basan, A; Makarevich, O. 'Evaluating and detecting internal attacks in a mobile robotic network'. International IEEE Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Zhengzhou, China, 2018.
12. Okuri, M; Higaki, H. 'Intentional collisions for preventing illegal overhearing by eavesdropper node in wireless sensor networks'. Second IEEE World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 2018.
13. Lambert, C; Völp, M; Decouchant, J; Esteves-Verissimo, P. 'Towards real-time-aware intrusion tolerance'. IEEE 37th Symposium on Reliable Distributed Systems (SRDS), Salvador, Brazil, 2018.
14. Guo, H; Meamari, H; Shen, C. 'Blockchain-inspired event recording system for autonomous vehicles'. 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 2018.
15. Sentsov, A; Polyakov, B; Gladkii, A. 'Electronic methods to protect unmanned aerial vehicles from seizing control'. IEEE Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 2018.
16. Zanero, Stefano. 'When cyber got real: challenges in securing cyber-physical systems'. 2018 IEEE Sensors, New Delhi, India, 2018.

*The Firewall*

# Goodbye SIEM, hello SOARX

**Colin Tankard, Digital Pathways**

Security information and event management (SIEM) technologies have, to date, been leading the war against cybercrime. They have provided a way to manage, correlate and deliver context from the many alerts generated by normal and abnormal network activities. But they have limitations.

Many SIEM systems are complimented by a security orchestration, automation and response (SOAR) package that aims to leverage the power of automation to add consistency in operational security processes and provide cost savings and efficiencies in the way security operation teams, or security operation centres (SOCs), are managed. The end goal is to reduce the number of alerts, significantly increase efficiencies and gain huge improvements in mean time to detect (MTTD) and mean time to respond (MTTR) to cyberthreats.

But SIEM systems can't handle custom applications and do not follow standard command APIs. Most do not report on breaches in such systems, leaving networks with blind areas. Trust is also an issue. Do you trust these systems to automatically shut down servers? What if it is your reservations server and you are booking clients at peak times, for instance?

We have all seen the slow uptake of intrusion detection and prevention systems (IDS/ IPS), with IPS still being throttled due to its high false-positive rate. Lack of trust in its decisions to take action and lack of flexibility mean it is not fully deployed, or in many cases, removed from a network.

However, given that threats to organisations are coming from many different directions – together with multiple layers of data security systems in play – now, more than ever, the situation dictates the need for a system that can look at the complete structure, one that can drill through the layers and unify the threats into a single view. It should have the built-in ability to take appropriate action, based on business dynamics appropriate to the threat, stopping the attack from happening in the first place.

The latest move to solve this issue is a totally new approach – SOARX, a solution that offers a central management offering for security orchestration, automation and response, going beyond existing SOAR offerings due to its ability to fully manage, monitor, automate and orchestrate complex network and security ecosystems from a single pane of glass. This works not only for known applications or devices, but also custom-built applications, legacy devices and cloud-based services, both public and private.

Applying business logic to the findings of the system enables proactive actions to be taken that can be linked to the level of threat on a particular application or device. For example, a threat to a bookings system can be graded. This would mean that, given a low threat level, the system would not be taken offline, resulting in loss of revenue. Old-style IPS systems had only an on/off approach.

Using the platform for the migration of systems and devices is another benefit. Switching from one load balancing company to another, for example, is normally complicated, fraught with potential errors and downtime. But with a SOARX approach, configurations can be replicated while both systems are in place and working together. Once the new system is deployed and signed off, the old system can be taken offline, by SOARX, in a controlled way.

At last there is a system to truly manage our complex network of systems and applications, which is not bound by 'standard' communications but is a platform that enables organisations to have a much greater view of their world and make decisions based on real information.

# EVENTS CALENDAR

14–15 November 2019
**DevSecCon London**
London, UK
www.devseccon.com

20–22 November 2019
**International Conference on Cyberlaw, Cybercrime & Cybersecurity (ICCC)**
New Delhi, India
http://cyberlawcybercrime.com

26–29 November 2019
**DeepSec**
Vienna, Austria
https://deepsec.net

9–11 December 2019
**World Congress on Internet Security (WorldCIS)**
London, UK
www.worldcis.org

9–11 December 2019
**International Conference for Internet Technology and Secured Transactions (ICITST)**
London, UK
https://icitst.org

11 December 2019
**FutureCon Nashville**
Nashville, TN, US
https://futureconevents.com/events/nashville-tn/

6–9 January 2020
**FloCon**
Savannah, GA, US
http://bit.ly/2Spye0d

28–30 January 2020
**FIC 2017**
Lille, France
www.forum-fic.com

4–5 February 2020
**PrivSec**
London, UK
https://london.privsec.info