

The State of Industrial Cyber Security 2019

July 4th, 2019

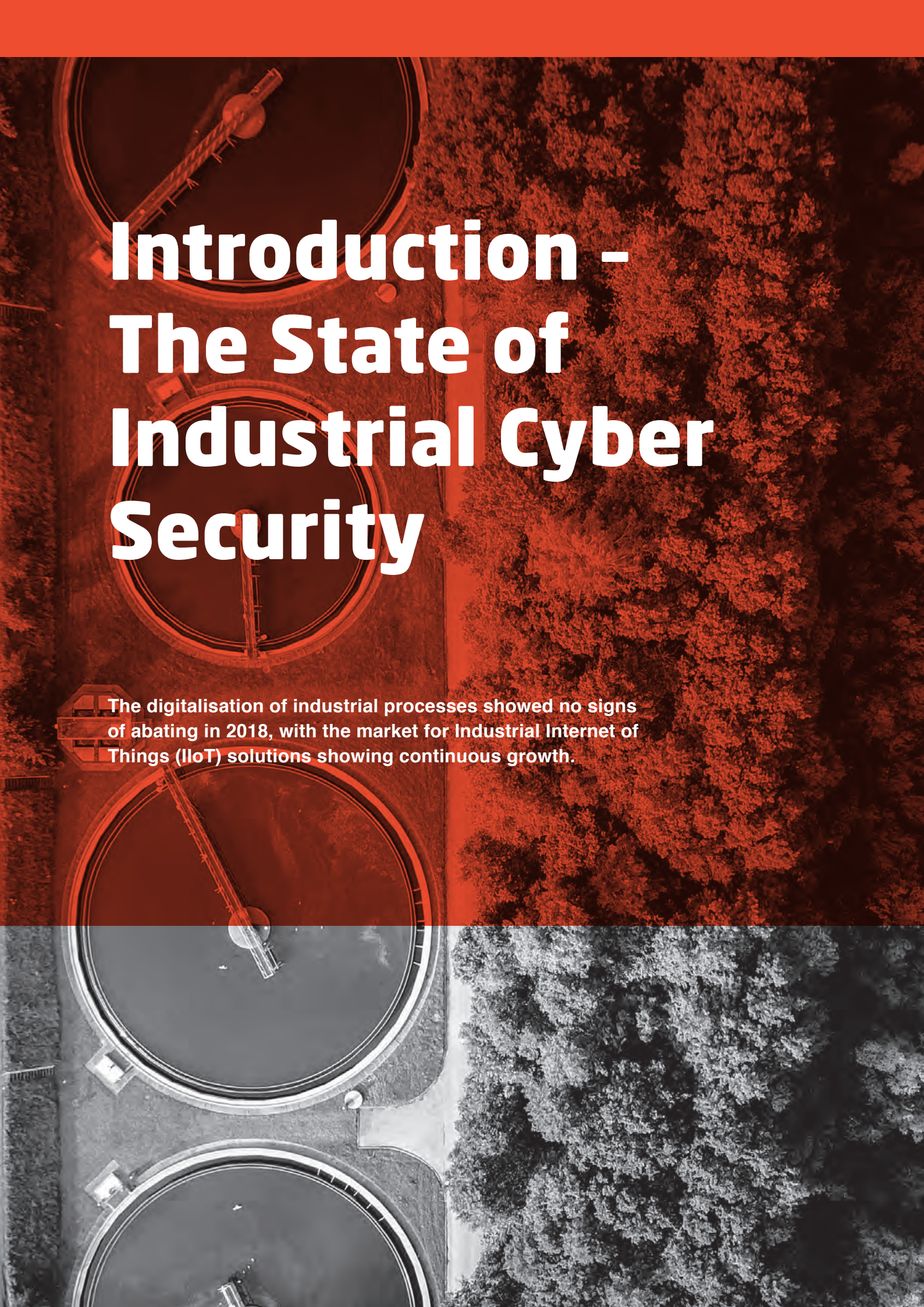


**Applied
Risk**



Index

Introduction	3
Executive Summary	4
Trends in Industrial Cyber Security	7
Attacks in the OT Domain	9
Field Operations	14
Recommendations	23
Final Thoughts	28
Appendix	26



Introduction - The State of Industrial Cyber Security

The digitalisation of industrial processes showed no signs of abating in 2018, with the market for Industrial Internet of Things (IIoT) solutions showing continuous growth.



Industrial automation processes are being made more efficient thanks to the collection and analysis of data from IIoT devices. Automation is moving beyond the simple mechanisation of repetitive tasks and into the realm of AI-led decision-making.

In the world of operational technology (OT), processes ruled by Industrial Control Systems (ICS) were traditionally designed with a strong emphasis on physical security and functional safety, but with little regard to the dangers of the online world. By virtue of not being connected, they were protected from malware and other destructive attacks distributed via networks and the Internet.

Our research shows that those who are responsible for the cyber security of OT are waking up to the challenges that digitalisation brings. Media coverage of the issue is growing thanks to the increased awareness of attacks, and high-profile global companies are therefore showing themselves to be more willing to disclose and report to competent authorities regarding incidents. Geopolitical tensions have also helped to highlight the level at which state actors are willing to engage in cyber attacks to further push their agendas.

At the same time, regulators are also helping to bring the security agenda to the fore, with better guidelines and laws covering OT. In the European Union (EU), the Directive on the security of network and information systems (NIS Directive) came into force in 2018, followed a month later by the Critical Information Infrastructure Protection Regulation (CIIPR) in China. As the year closed, similar legislation was also being considered in countries such as Canada, Qatar, Russia and South Korea. These legislations offer both best practice guidelines and advice for those who want to be proactive, and the threat of fines, reputational damage or worse for those who don't.

Applied Risk strongly believes that cyber security can no longer be treated as an afterthought within industrial environments. By placing it at the heart of their practice and culture, it can deliver real business benefits, mitigating the risk of operational, financial and reputational damage. It can deliver competitive advantage as end customers demand more transparency from their own supply chains. And most of all, it gives organisations the confidence to embrace the opportunities that the digitalisation of industrial environments and IIoT present, while containing the risks that they pose.

This report is designed to help those who manage industrial environments to do just that, and develop a clear understanding of the trends, risks and opportunities of digitalisation. In it, we analyse our own field research and learnings from dealing with customers in live environments to identify the most common areas of vulnerability that we see in OT deployments, and offer our own advice for addressing them.



Executive Summary

This report represents a combination of insights from the Applied Risk team, alongside data-driven learnings from analysis of work with customers and findings from internal research teams over the past 12 months. It also contains an overview of known vulnerabilities, drawn from publicly available databases, which can affect ICS and IIoT technology.

The report identifies trends which affect cyber security in industrial environments and includes some insight as to their causes, effects and future implications.

Key trends within the industry:

- Greater public awareness of issues around industrial cyber security
- Closer integration of OT and IT systems
- The rapid proliferation of new and untested technologies
- An increase in the number of cyber security regulations around the world
- The growth of cyber insurance
- The shortage of industrial cyber security skills

Drawing directly on our work testing and implementing security strategies for customers, we have identified the top five technical and the top five non-technical issues to industrial cyber security. Our findings suggest that the cyber security basics are still not regularly practised in organisations with an OT environment.

Top five technical observations

- 1 Outdated and vulnerable software**
Vendor support for older systems is ending too early, and there's a general failure on behalf of OT managers to implement firmware upgrades where they are available and possible to implement.
- 2 Inadequate network segregation**
Segmentation in the OT domain is critical, but inadequate. Furthermore, firewalls are often sub-optimal, and there are weak boundaries between OT and IT environments.
- 3 Lack of system hardening**
We identified that a lot of device installations had minimal hardening measures implemented, if at all.
- 4 Weak access control**
Access control in both the physical and digital sense is often poorly managed and can undermine the security controls that have been set in place.
- 5 Insufficient logging and monitoring**
Systems should be monitored in real-time for unusual behaviour, and system logs can help with forensics post-attack.

Top five non-technical observations

- 1 Governance**
Overall governance of cyber security in OT is low. Company-wide policies, regular risk assessments and security planning are all notable by their absence.
- 2 Staff training and security awareness**
Human error or unqualified personnel is still the primary cause of security breaches, and employers must provide regular training to help staff change insecure behaviour.
- 3 Business continuity plan**
There is a lack of definition of roles and responsibilities among personnel in the event of an incident. Having such definitions in place and well communicated throughout the operational staff can make a real difference in reducing the impact of incidents when they take place.
- 4 Third party management**
Many site operations rely on suppliers of systems to implement and integrate security, yet there are often no formal agreements with these suppliers to ensure these products are secured by design.
- 5 Incident response planning**
A detailed incident response plan that includes documented processes for isolating the cause of an incident and taking appropriate steps to restore operations is vital if an organisation is going to mitigate the amount of downtime, data loss and reputation damage from an incident.

While this is, of course, concerning, the good news is that asset owners and suppliers are now in a better position to prioritise risk and address it accordingly.



Trends in Industrial Cyber Security

The digital transformation of industrial processes shows no sign of slowing over the next five to 10 years, but attitudes, awareness and the risks associated with industrial cyber security in OT are constantly changing. Applied Risk has identified six predominant trends that influence this.

1. Industrial cyber security in the news

Awareness of cyber security in the world of consumer and corporate IT has risen dramatically in recent years, as a result of several well-publicised and analysed attacks which have the ability to disrupt essential services in health and telecommunications on a national scale. Awareness of attacks on industrial environments are also starting to make headlines. Caution should be taken to distinguish between facts from trustworthy sources and Fear Uncertainty Doubt (FUD).

To disclose or not to disclose?

Cyber security incidents in OT aren't as common as those in the IT world, but they are being more widely reported on and their potential for damage is better understood.

Some organisations have helped thanks to their willingness to disclose attacks. For example, many companies have revealed that their operations were disrupted by a variant of the NotPetya malware. In other cases, researchers have helped to keep the issues in the news. The TRITON malware, which targets the family of Triconex Safety Instrumented Systems (SIS) has also been covered extensively¹.

2. Closer integration of OT with enterprise and business systems

Digital transformation of industrial activities has led to a further blurring of the lines between OT and IT networks. Historically, OT systems may have been segregated from the outside world, but that no longer exists as the IP network becomes pervasive. The need to collect, analyse and act upon data collected from the OT domain means that we can expect more resource pooling in the future, as new methods of processing information at the network edge continue to cross boundaries between OT and IT.

3. New technologies find their way to OT

Automation no longer means the mechanisation of processes. It means placing machine learning and AI at the heart of the decision-making process. This in turn requires data to be transmitted from the OT environment for processing in the cloud. For example, more solutions are being deployed that are reliant on AWS, Azure etc. The data being sent to the cloud can be Confidential and/or Sensitive and could lead to reputational damages if disclosed (maliciously or non-maliciously).

Depending on where this data is processed, connected devices may be vulnerable at points outside the OT manager's control. Often, they are deployed without correct testing and hardening, providing attackers with an entry point that bypasses traditional points of security, creating vulnerabilities in systems thought to be well protected.

Despite increased awareness, new technologies are still regularly deployed in a manner that prioritises speed of implementation over security considerations, without a full "secure by design" process.

4. Laws and regulations coming into place

Lawmakers around the world are waking up to the danger posed by poor cyber security in OT for public health and safety. In the European Union, for example, the NIS Directive began being transposed into local laws in 2018, giving those involved with critical infrastructure clear rules for governance. Although it

has been adopted by some EU states, there are many which have missed the deadline for incorporating it into national law².

The Chinese government also published its own Critical Information Infrastructure Protection Regulations (CIIPR), and other initiatives are under way in Russia, Singapore, South Korea and throughout the Middle East.

5. Cyber insurance

Awareness of the risks and the potential for financial harm that a cyber security incident can cause has led to a sharp rise in demand for and provision of specialist cyber security insurance policies. Typically, these are designed to cover costs for responding to and investigating attacks, as well as damages incurred. Many policies are currently untested, however, and areas of coverage may be unclear.

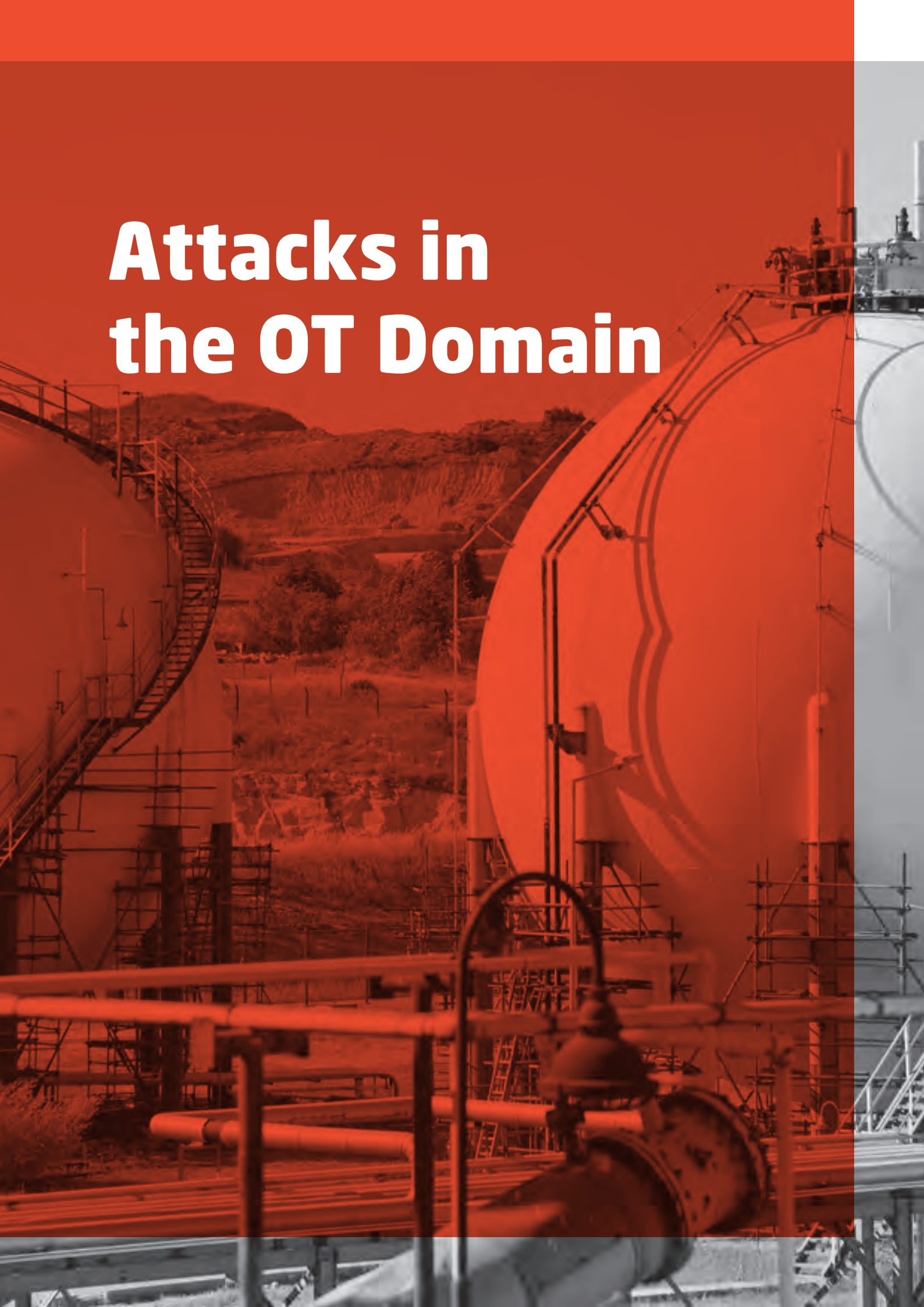
6. Shortage of industrial cyber security skills

There's an acknowledged shortage of ICS cyber security specialists worldwide. This shortage is compounded by the complexity of the environments in question, which are generally non-homogenous and upgraded in an ad hoc manner. The longevity of industrial equipment increases the likelihood that legacy and unsupported systems will still be part of the operational mix, increasing the challenge for protection.

"We were struck by the Government's apparent lack of urgency in addressing the cyber security skills gap in relation to CNI (Critical National Infrastructure). CNI operators and regulators told us that the shortage in specialist skills and deep technical expertise is one of the greatest challenges they face in relation to cyber security. In particular, there is an acute scarcity of experts who understand the security implications of connecting often bespoke or legacy CNI control systems to the Internet."

- The Joint Committee on the National Security Strategy, UK Parliament³

Attacks in the OT Domain





The complexity of OT environments means that implementing effective cyber security requires analysis and planning. For this, organisations must be able to evaluate and map the risks to an industrial process, use these to consider the potential consequences of an incident taking place and determine effective mitigations to lower the likelihood of the incident taking place or minimise its impact on industrial processes.

How do attackers get in?

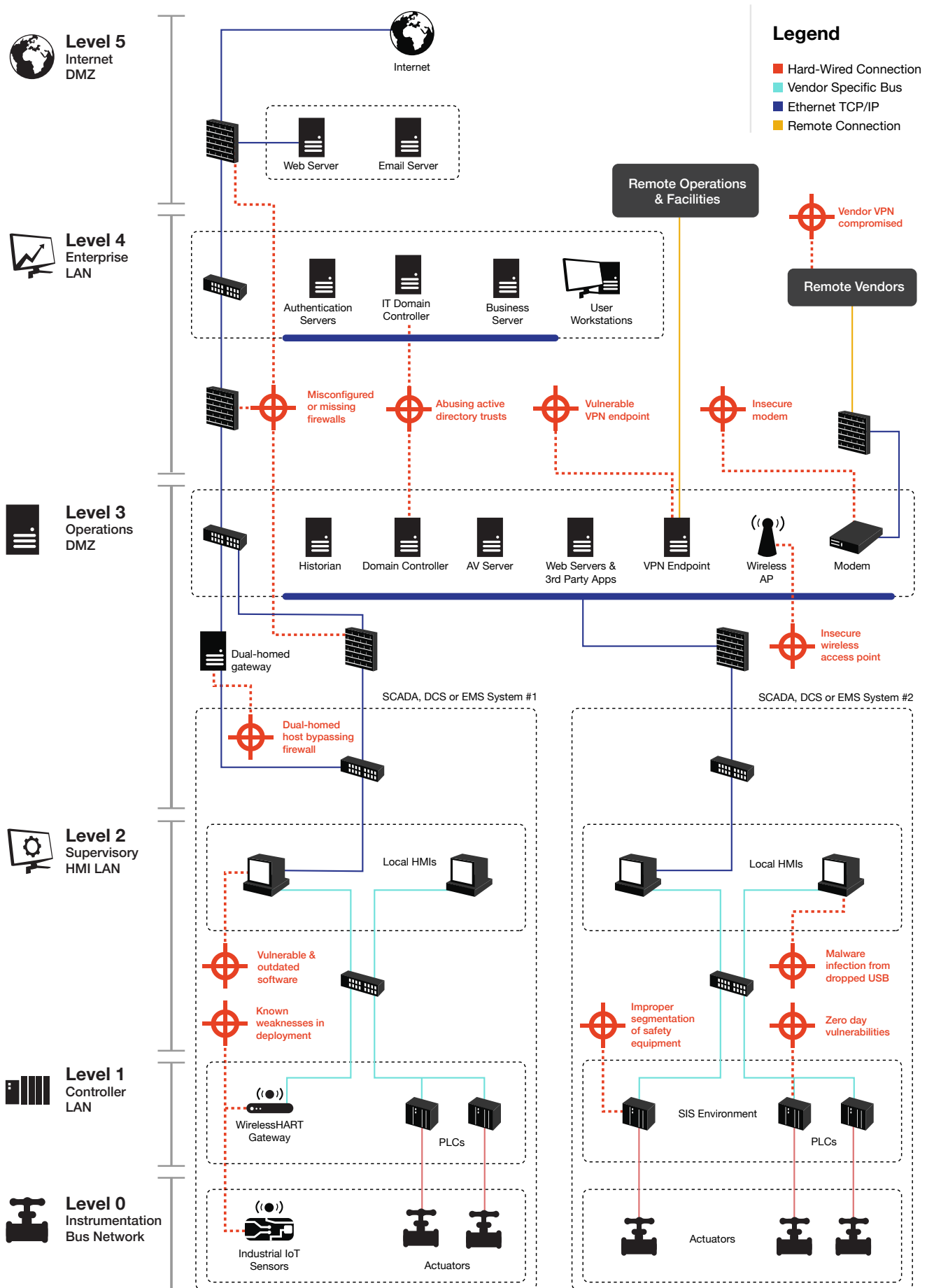
Traditional OT security has relied on air gapped networks for ICS and SIS, or firewall protection at the perimeter. The complexity of today's environments undermines these approaches, and while traditional firewalls are far from obsolete, they cannot be the sum total of a firm's cyber security efforts, and additional security mechanisms such as uni-directional traffic, white listing, anomaly detection and next-generation firewalls are strong supplementary security controls.

This diagram shows a typical network topology for an OT environment today and illustrates multiple entry points that are vulnerable to attack. Not all organisations will have the same risk factors, but generally it's clear that this network is exposed at several points.

To disrupt an industrial process, an attacker would need to take over key control systems. This could be achieved in several different ways, highlighting the need for a "defence-in-depth" strategy that employs multiple levels of protection, including layered networks, strong access control, system hardening and regular testing of all entry points.

Attack Vectors

This diagram depicts a number of attack vectors that attackers typically can use to pivot through an OT environment, mapped to their corresponding level in the Purdue model.



Vendors

Firmware or software that “phones home” for vendor services, remote control or support is an obvious weakness if attackers are able to compromise the vendor’s infrastructure or VPN or obtain their VPN credentials. Likewise, not all vendors have adequate ICS security skills and code may not be properly tested for vulnerabilities or written with security standards in mind.

Remote operations

There’s increasing demand for remote access to OT, either to support staff mobility, or geographical deployment, or to allow for third parties to conduct preventive maintenance.

IT/OT integration

Speed to market and price sensitivity too often trump security when developing IIoT sensors and networks. Security is expensive, and profit margins are low – untested devices with outdated firmware and known exploits can still be found on the market, and are often deployed, even in highly sensitive environments.

IIoT sensors and gateways

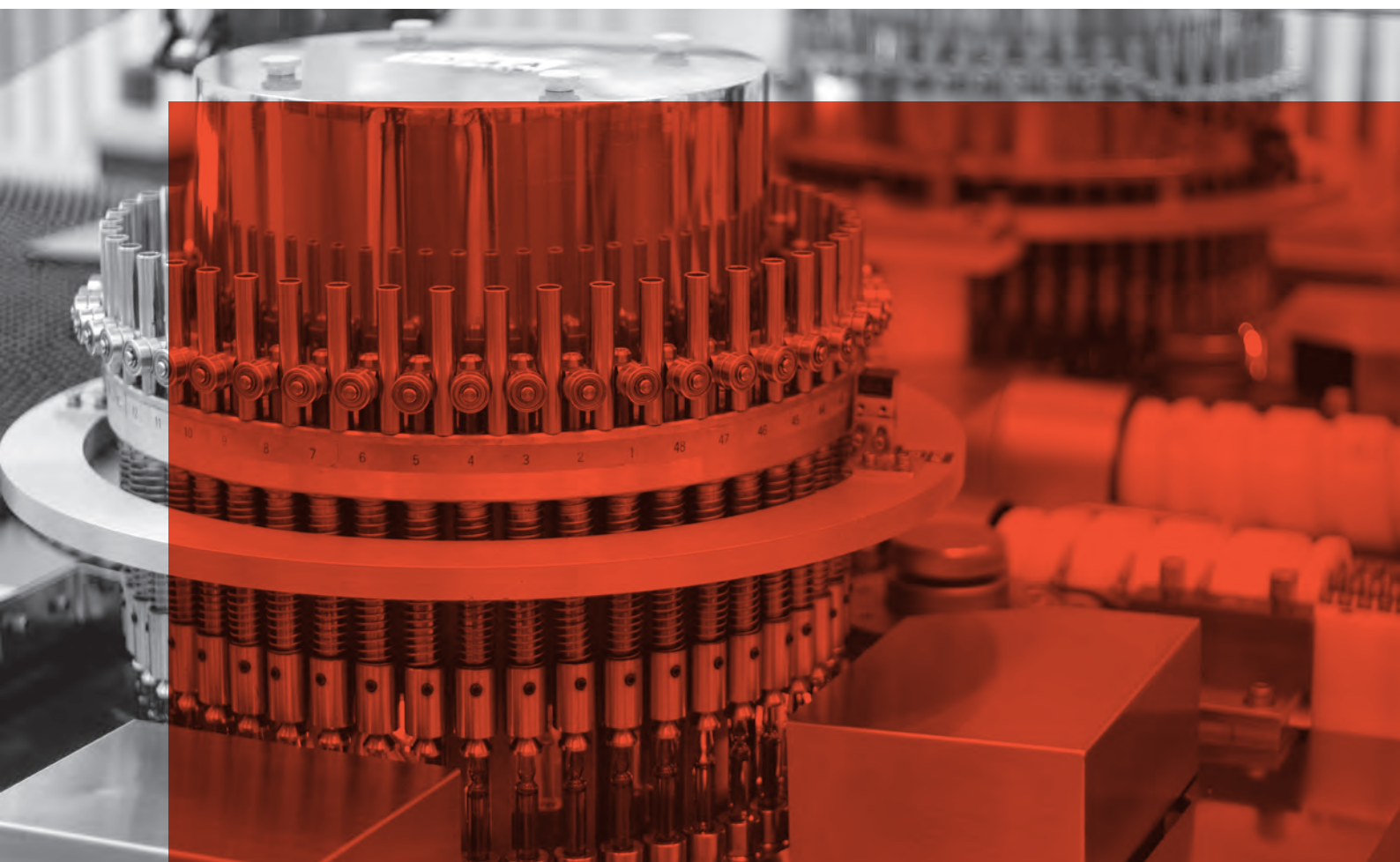
Speed to market and price sensitivity too often trump security when developing IIoT sensors and networks. Security is expensive, and profit margins are low – untested devices with outdated firmware and known exploits can still be found on the market, often in highly sensitive environments.

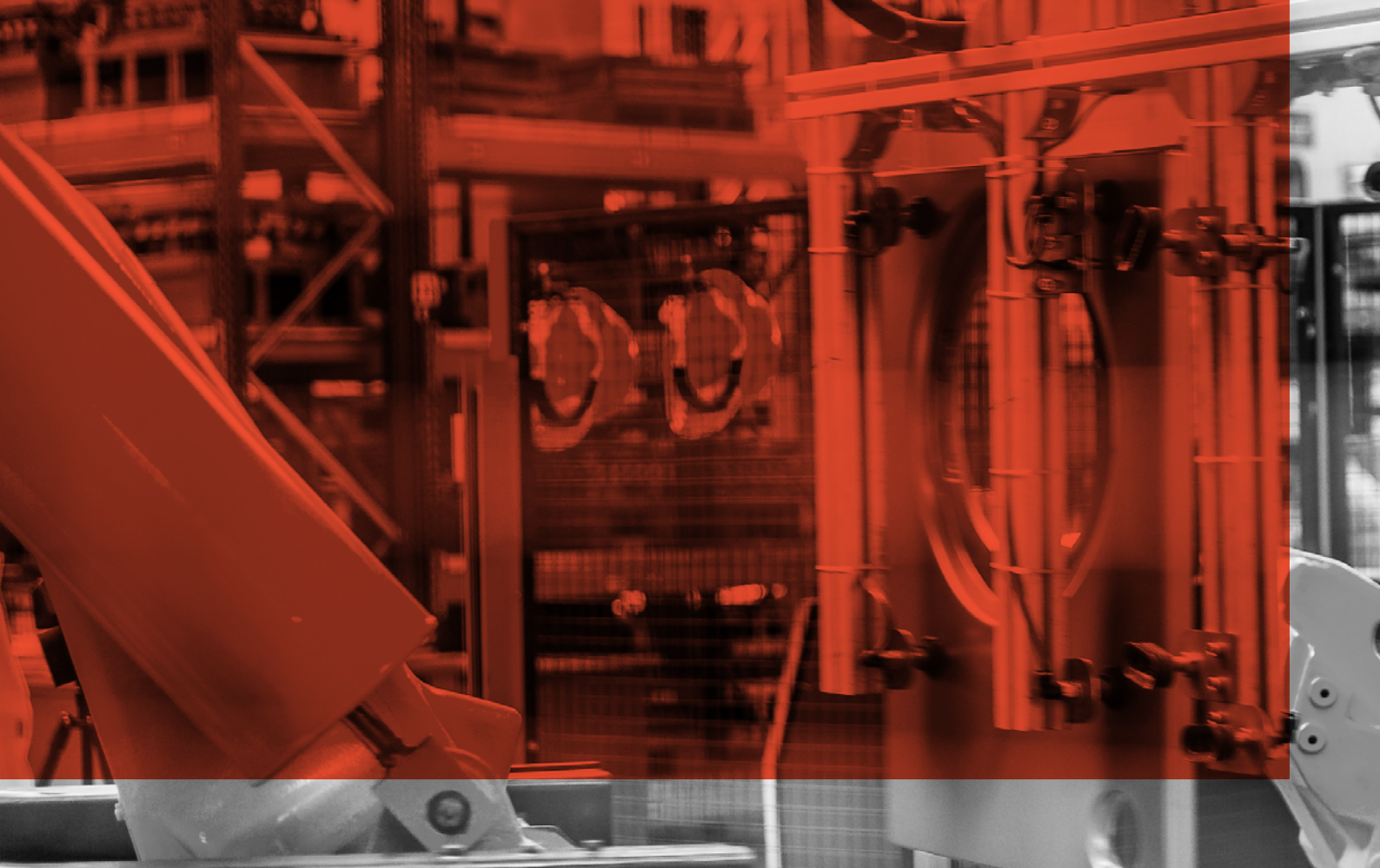
Malware infection from removeable media

Malicious or unwitting employees may infect workstations connected to the OT network using USB devices, DVDs, laptops and more, providing a backdoor for an attacker or resulting in virus/ ransomware outbreak.

Poorly configured access points and modems

Default credentials and open ports leave systems exposed to the Internet. Many industrial devices show up in the records of SHODAN, a search engine which catalogues devices that are directly connected to the Internet and therefore potentially at risk. Worms such as “Hide and Seek” (HNS) exploit this exposure by looking for IoT devices that they can take over.





Targeting safety systems

Safety Instrumented Systems (SIS) are critical parts of an OT environment, usually designed to take control and manage the shutdown of processes in the event of an incident which threatens physical safety. They present a particularly concerning target for bad actors, as controlling a SIS can disrupt operations or prevent them from functioning, which could result in physical damage through an explosion or fire, posing a potential risk to life.

2018 was notable for the discovery of the TRITON malware, which targets Schneider Electric's Triconex SIS. The Triconex system is widely used in the energy sector and in power stations, and the TRITON malware has been discovered in one industrial plant in the Middle East, targeting vulnerabilities in widely used safety systems. Failure to correctly isolate SIS from the wider network or apply vendor-supplied security patches exposes them to these threats.

“Digital safety systems suffer from the same fundamental problem as basic production controllers. They are insecure by design. In today’s hyper-connected networks, safety systems require extra scrutiny by cyber security experts.”

Ralph Langner, CEO, Langner Inc.

Supply chain attacks

Companies that supply software and managed services to clients have also been targeted and the assumption is that, by creating backdoors and placing payloads in commercial applications, bad actors can create an entry vector in multiple client sites. Many of these supply partners are part of a trusted network, and end customers may not be engaging in full due diligence by commissioning an independent security audit of their product before deployment.

In cases where remote access is deemed necessary, measures should be taken to isolate their access properly and ensure they only have access to what is necessary. Furthermore, these connections should be actively monitored to detect any signs of malicious or unusual activity.

Field Operations

Methodology

Applied Risk carries out many security assessments every year on behalf of clients around the world. For this report, our findings are based on the collated results of our assessments carried out in 2018, identifying a total of 768 unique findings.

The types of assessments we conduct include:

- OT Penetration Testing
- OT Health Check Assessments
- OT Design Architecture Reviews
- OT Risk & Compliance Assessments
- OT Asset Discovery
- OT (Vulnerability) Lab Security Research

We have also included analysis based on the evaluation of publicly available, ICS-specific CVE data over the period 2016-2018.

Sectors in scope:



Oil and gas



Power



Chemical



Manufacturing



Water



Pharmaceuticals



Maritime



Transport



Mining

Top five technical observations

Technical findings are based on data from our technical services and research. Based on this data, the most prominent issues that we see are:

1

Outdated and vulnerable software

The primary challenge we see in the field is poor patch management and the use of unsupported software. This leaves the door open for attackers with off-the-shelf tools, who can exploit weaknesses easily. In the IT sector, this practice was directly responsible for the spread of the WannaCry ransomware that crippled many organizations. In 2018 and 2019 other ransomware campaigns also directly impacted industrial sectors.

These systems should be upgraded, replaced or properly isolated to communicate with only what is explicitly necessary.



Common issues found:

- End-of-life operating systems and equipment in use such as Windows XP
- Lack of patches
- Custom web applications running on outdated web servers
- Outdated firmware versions on embedded Linux devices
- Insecure by design Level 1 devices

2

2. Inadequate network segregation

Attackers seeking to gain control of OT through the network are well versed in the technique of exploiting poorly configured gateways and other equipment to leverage weaknesses in the IT network to reach the OT environment. Poor segregation of sub-systems within the safety and control networks is also an ongoing issue.



Common issues found:

- Safety Instrumented Systems (SIS) not properly segregated from the rest of the OT network.
- Safety systems (which should be in Level 1 in the Purdue model) that are accessible from OT assets in Level 3. Therefore, an attacker could compromise safety engineering workstations and conduct attacks against the SIS.
- Though we find firewalls deployed, in many cases their efficacy is undermined by poor rulesets that fail to restrict traffic to the specific hosts that need to communicate with each other and protocols required for operations.

Applied Risk recommends segmenting the network according to the 'Zones and Conduits' model as proposed in the IEC 62443, whereby assets are grouped into logical or physical assets that share common security requirements based on factors such as criticality and consequence (security levels). The connections between these zones are called conduits and must include security measures in order to control access, resist Denial of Service (DoS) attacks, prevent the spreading of other attacks, act as a shield for other systems in the network and protect the integrity and confidentiality of communications.

3

Lack of system hardening

Vulnerabilities are created in systems when access credentials are left in their default state or insecure protocols or permissive services are left in use.



Common issues found:

- Instances where OT server clocks aren't synchronised (NTP), which can reduce the effectiveness of encryption and hamper the efforts of post-event forensics.
- Weak network management and authentication strings in use, based on old protocols that are known to be vulnerable.
- Unused features and functions are not disabled, contrary to best security practice for locking down devices to only their intended use.
- A lot of device installations had minimal hardening measures implemented, if at all.

With some vendors, patches and updates may be unavailable. In such situation, it is necessary to plan for upgrade, migrate, or isolate the system from network to minimise likelihood from cyber risks.

4

Weak access control

Access control in both the physical and digital sense is often poorly managed and can undermine the security controls that have been set in place. Managing joiners and leavers, account permissions and weak passwords, which are frequently encountered during engagements, could be resolved by establishing and enforcing a strong password policy.

However, the storage of passwords also needs consideration as a strong password is of no use if it is stored on an unencrypted system that is accessible to other users. In addition, the principle of "least privileges" should be applied across the organisation - that is to say, restricting the permissions of user accounts to only those which they require

and no more. Failure to implement such measures assists attackers who are able to gain access to accounts to potentially pivot between systems in the network.



Common issues found:

- Default credentials in use
- Credentials stored in plaintext documents
- Missing Network Access Controls (NAC)
- SSH keys not password-protected
- Lack of privileged access management
- Guest accounts enabled

5

Insufficient logging and monitoring

An important lesson from recent developments in the IT world is that one of the most effective ways to spot new and evolving threats is through host-based monitoring, such as with Endpoint Detection and Response (EDR) tools. Such tools can facilitate effective incident response processes (e.g., through being able to perform host iso-lation).

For some OT systems, however, host-based monitoring is not an option, and this issue is compounded in that many also only store data in volatile memory, and a lack of accessible logs hampers both threat awareness and the ability to perform forensics once an incident has taken place. Network monitoring in such situations can be of benefit, and while passive and active monitoring tools are available for OT environments, this is an area which is seeing vast improvements.

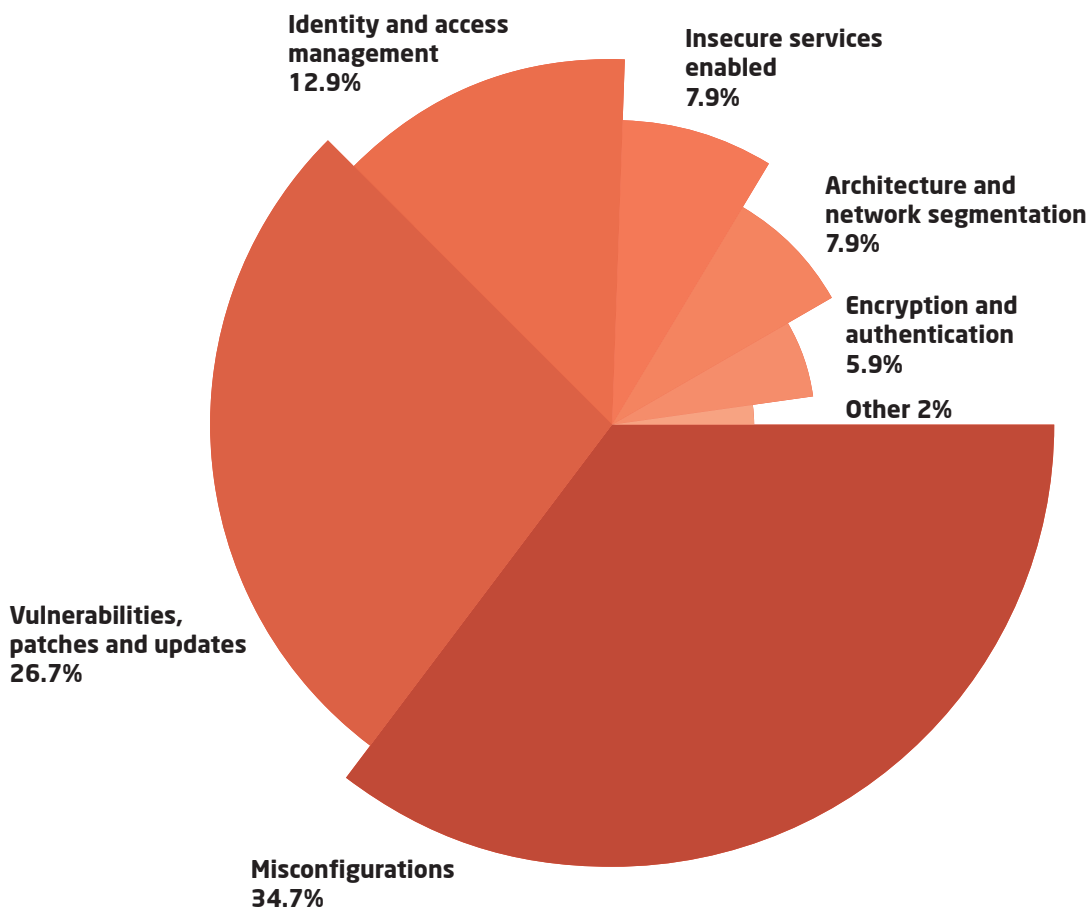


Common issues found:

- Monitoring tools rarely utilised in OT environments
- No logs available, hampering threat awareness

Technical Findings by Category

An analysis of technical observations used to visualise the most common types of vulnerabilities within industrial control systems.



Simple, but effective

The good news is that the most common issues we see are all relatively easy to fix. It doesn't take much work to upgrade the overall security posture of organisations. This is not a one-off fix, however. The key to sustainable cyber security is to ensure there are people directly responsible for maintaining security in the OT domain.

Top five non-technical observations

These observations are less technical in nature, and are derived from our risk and compliance oriented services:

1

Governance

Overall governance of cyber security in OT is low. Company-wide policies, regular risk assessments and security planning are all notable by their absence. It's a cliché, but in these environments the need for good governance in personal safety is well understood and accepted as paramount; the same considerations must also be applied to cyber security.

A lack of clear definition of the roles and responsibilities within the organisation when it comes to making security-related decisions can reduce the overall impact of a cybersecurity framework. Not to be confused with IT management, cyber security governance focuses on longer-term strategic decisions rather than short-term tactical decisions.



Common issues found:

- Lack of clearly defined roles and responsibilities within management to address cyber security strategy
- Lack of funding for roles in run & maintain organization
- Lack of OT-specific security policies and procedures
- Lack of risk management methodology translating OT security issues into business impact

2

Staff training and security awareness

The weakest point of any cyber security plan is always the human being. Human error or ignorance is still the primary cause of security breaches, and employers must provide regular training to help staff understand the need to be vigilant in all aspects of their work and change improper behavior jeopardizing cyber security.



Common issues found:

- Printed passwords displayed on sticky notes and paper
- Sensitive documentation left unattended on desks
- Inappropriate storage of assets (e.g. network equipment left unattended in a hallway)
- Unlocked network cabinets

3

Business continuity plan

Cyber security incidents are, sadly, an inevitability of modern life. Reliable backups and disaster recovery scenarios can ensure continuity of operations when something goes wrong. Crucially, we see a lack of definition of roles and responsibilities among personnel in the event of an incident. Having such definitions in place and well communicated throughout the operational staff can make a real difference in reducing the impact of incidents when they take place. Performing regular exercises to test the business continuity plans is equally as important.



Common issues found:

- A general lack of a specific continuity plan
- Lack of a cyber security-specific plan, dealing with different types of attacks including advanced persistent threats and ransomware but also unintentional impact due to human errors or misconfigurations.
- Poor/absent definitions of roles and responsibilities in the event of an incident
- Back-up and restore not tested

4

Third party management

Many site operations rely on suppliers of systems to implement and integrate cyber security, yet there are often no formal agreements with these suppliers to ensure these services are delivered in a secure manner. This results in a lack of clarity

regarding the responsibility of security with the suppliers.

Additionally, security features that are available from the suppliers are not being utilised. Again, this is often as a result of failing to put the right agreements in place.



Common issues found:

- Lack of formal supplier agreements to ensure supply chain cyber security
- Little awareness of who is responsible for cyber security

5

Incident response planning

Having a detailed incident response plan that includes documented processes for isolating the cause of an incident and taking appropriate steps to restore operations is vital if an organisation is going to mitigate the amount of downtime, data loss and reputation damage from an incident. An incident response plan should include 24/7 availability of OT security stakeholders, including third parties, as well as regular exercises and planning for crisis scenarios in the face of a cyber security incident.



Common issues found:

- No 24/7 availability of OT cyber security in case of emergency or incident
- Undefined plan of action in the event of an incident
- No crisis scenarios/drills related to OT cyber security incidents regularly conducted

Insights from CVE data

Applied Risk has undertaken the research with a specific methodology. Over time, this approach will be expanded upon.

Only vulnerabilities contained with ICS-CERT advisories for the period 2016-2018 were considered, as well as vendors public data.

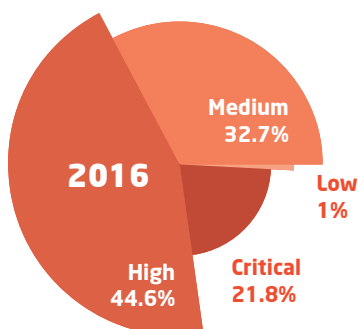
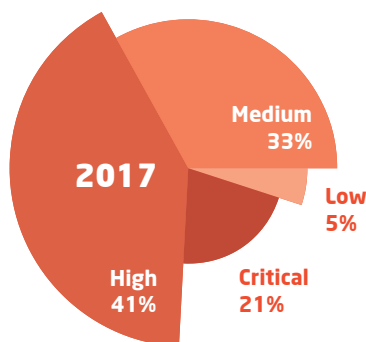
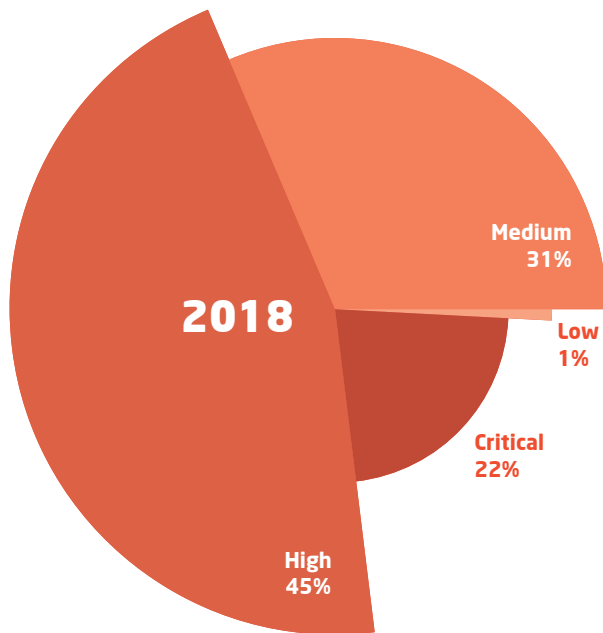
Essentially, being posted on ICS-CERT became the filter for OT-related vulnerabilities. In the future, this will also include other manufacturer-specific advisories.

“The threats to industrial control systems continue to increase each year. I urge organizations that use automation to ensure they are training their personnel, have risk mitigation plans in place, and practicing their disaster recovery procedures”

Marty Edwards, Former Director, ICS-CERT

Vulnerability Severity Levels by Year

An analysis of technical observations used to visualise the most common types of vulnerabilities within industrial control systems.



In total, Applied Risk identified 323 ICS CVEs for 2018. This dataset is large enough to be able to ascertain broader trends among the CVEs.

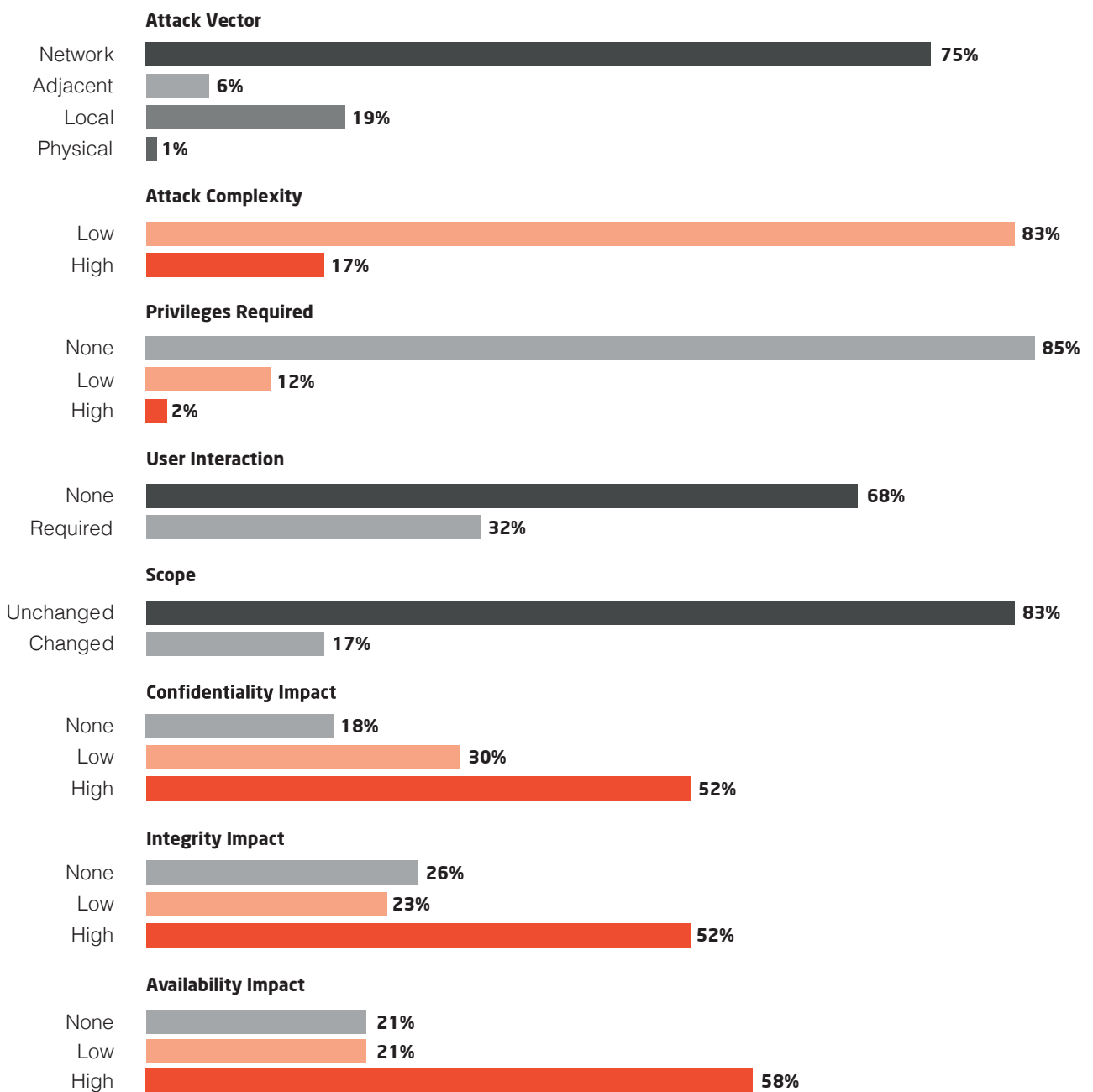
What we found was that:

- There was no real change in the severity level of CVEs in recent years.
- Nearly 70% of CVEs have a severity rating of High and Critical.
- 75% of vulnerabilities are exploitable over networks, with far fewer flaws requiring physical or local access to the target.
- Vulnerabilities tend to have low complexity – i.e. specialised access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.
- No special privileges are required for 85% of the CVEs.
- These vulnerabilities scored mostly “High” on the Confidentiality, Integrity and Availability (CIA) Index. They particularly affect Availability, meaning an attacker who exploits them could shut a system down completely.

The worrying take-aways from this are that vulnerabilities found in OT devices and software tend to be remotely exploitable, require limited or no privileges, have low complexity requirements to perform, and have a High or Critical impact on the availability of assets. Should an attacker manage to gain access to the OT network, it does not require much effort to cause availability issues and jeopardise industrial processes. This drives home the need to apply a layered security approach and diversify security controls, which protects the whole OT environment and not just individual devices.

Vulnerability Metrics in 2018

Based on CVSS v3 scores from ICS-CERT advisories



Recommendations

A person wearing a white shirt and dark trousers is holding a white hard hat. The background is a blurred outdoor scene with a building and a tower. The entire image has a strong orange-red color overlay.

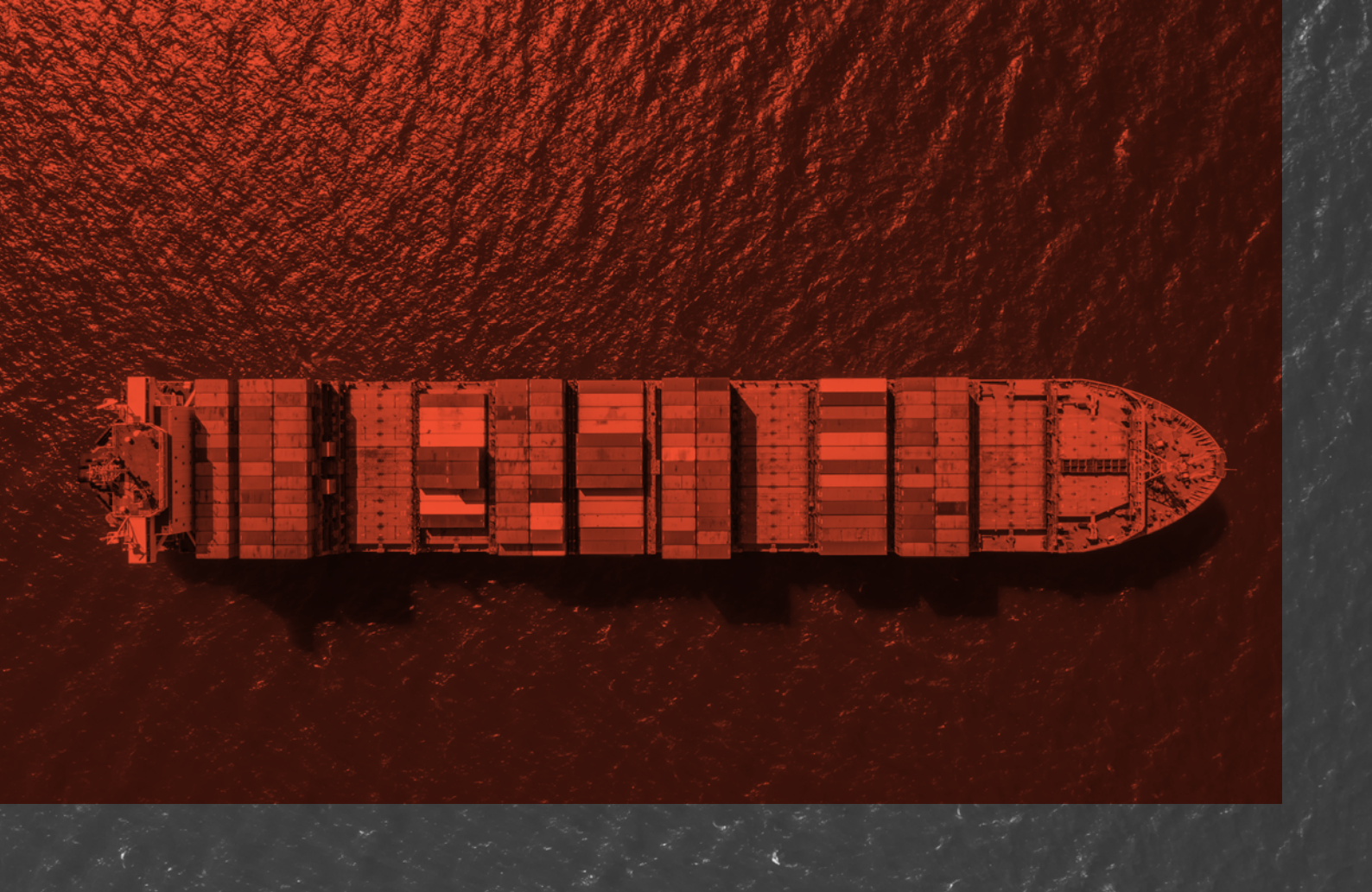
It is Applied Risk's conclusion that most common cyber security weaknesses already have known remedies. Therefore, well-established best practices can be quickly adopted, and that alone will deliver significant cyber security improvements in many organisations.



Asset owners

Managers of OT environments need to understand the critical importance of cyber security to their work and the potential impact on their business, from productivity and financial concerns, to reputational and environmental damage. The IIoT and convergence of IT and OT networks have created new opportunities for attackers, as well as the risk of unintentional incidents.

- The aim should be to be “secure by design”, which means ensuring that the cyber security of any system is a priority consideration right from the start of the procurement and design process and through to end-of-life considerations.
- It is essential that asset owners are more critical of vendors – even well-established ones – to ensure that their products and processes meet their own demanding requirements.
- In practice, this means working with trusted, vendor-neutral third parties to complete a full security audit and risk assessment of the existing environment and relying on the same independent advice to assess future integrations for vulnerabilities.
- The need for constant vigilance should encourage investment in an OT security run and maintained organization, including network monitoring and proper planning for incident response and maintenance.
- Organisations, together with their security partners, should be engaging in regular penetration testing, hardening and security drills. These should include collaborative attack simulations, and tests of incident response plans co-ordinated with vendor partners.
- Company cultures need to change to reflect the importance of cyber security at all levels. Staff awareness programmes need to come out of the induction process and become regular features integrated into Key Performance Indicators.



Vendors and System Integrators

The Secure Development Lifecycle (SDLC) process is a proven model from enterprise application development which places cyber security at the very heart of any new product or service, right from the beginning of the development pipeline. Vendors should adopt the same approach to OT components, modelling potential threats and building in safeguards to mitigate against them.

- SDLC processes should be thoroughly documented so end products can be validated against design.
- Better distribution systems for patching and firmware updates should be in place.
- More investment should be made into the adoption of applicable accreditations for vendors to demonstrate their commitment to cyber security and help customers understand the need for these certifications. Much work has been put into ISASecure and IEC 62443, for example, which should be recognised.

The Bowtie Model for Risk Evaluation

The challenge of securing complex industrial environments from cyber security threats requires a multi-faceted approach that can be difficult to visualise and develop pragmatic controls for. To this end, the Bowtie model can be an effective tool for achieving this.

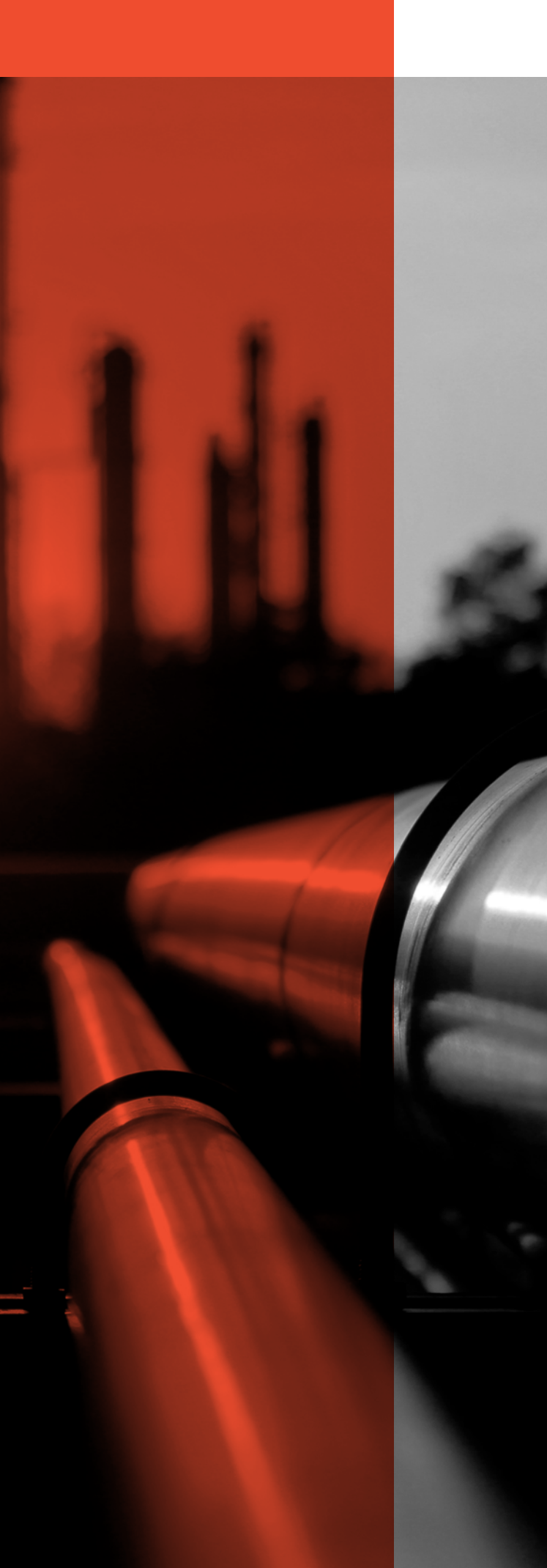
By plotting the specific threats leading up to an event and the resulting consequences, it becomes easier to plan and incorporate effective controls to either prevent the event from taking place or limit the consequences in case it occurs.

The Bowtie Model



Final Thoughts

The overall findings from this report should be taken in a positive manner. While it is clear that there is work to be done before we can say the majority of OT environments are suitably secure, effective risk management and cyber security are achievable goals for OT operators.



No environment is ever 100% secure, but in many of the cases that Applied Risk studied in 2018, there are proven and well understood interventions which can raise the level of protection dramatically.

The mission ahead of us is to increase awareness of the importance of effective cyber security in industrial applications. There will always be those vendors and integrators for whom speed to market and implementation are more of a priority than cyber security, but end customers can and should demand better, recognising those who have invested in appropriate certifications.

While awareness levels are rising, however, many of the challenges that are observed in the field come down to the fact that the skills for risk assessment and security hardening are in short supply.

For this, and many other reasons outlined in this report, cyber security isn't something one company can achieve alone. Supply chains have to be vetted and trusted; even a solution provided by reliable vendors may create vulnerabilities due to poor implementation.

Independent partners, trained and equipped with the right toolkits to test, harden, advise and secure OT in the field are essential to provide effective cyber security.

There is true business value in this method. In the future, Applied Risk believes that a proven, actionable approach to cyber security will be a competitive advantage to firms. Ultimately, as much as any organisation cares about cyber security, they will never care about it as much as their customers do. That said, the ultimate aim is that they must do.

Appendix

References

¹<https://threatpost.com/understanding-triton-and-the-missing-final-stage-of-the-attack/134895/>

²<http://ecdl.org/ecdl-news?i=3258>

³<https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf>





Disclaimer

This research utilises public information and has been published for information purposes only. Whilst every effort has been made to ensure the accuracy of the information supplied, Applied Risk cannot be held responsible for any errors or omissions.

This material may not be reproduced or distributed, in whole or in part, without the prior written permission of Applied Risk.

Copyright © 2019 Applied Risk BV. All rights reserved.



**Applied
Risk**

About Applied Risk

As a trusted partner for industrial cyber security, Applied Risk is driven to safeguard the critical infrastructure our society depends on. Combining cyber security knowledge and experience in operational technology, Applied Risk provides tailored solutions that assist asset owners, system integrators and suppliers to develop, deploy and maintain cyber-resilient operations. Based in the Netherlands, Applied Risk operates on a global scale, helping protect industries such as oil and gas, power, water management, manufacturing, healthcare, maritime and transport. To learn more, visit www.applied-risk.com

Applied Risk BV
Teleportboulevard 110
1043 EJ, Amsterdam
The Netherlands
T: +31 (0)20 833 4020
E: info@applied-risk.com
W: www.applied-risk.com