Business Advantage
intelligence insight innovation

The State of Industrial Cybersecurity 2017

GLOBAL REPORT

Contents

EXECUTIVE SUMMARY

The need to secure industrial control systems (ICS) from the risk of cyber-attacks cannot be underestimated in a world where human error, online criminal activity and espionage are very real threats to businesses.

The potential damage from cybersecurity incidents can be considerable. The consequences of these incidents are often far greater than the associated financial losses and reputational damage. Cybersecurity incidents in an ICS environment can:

- Cost lives
- Have a long-lasting impact on the environment
- Attract fines from regulators, customers or partners who have been put at risk
- Result in the loss of a product or service as a result of the breach
- Companies can close down completely

Certain organizations such as oil and gas companies have what could be defined as "critical industrial processes" with specific risk models due to the sensitive nature of their infrastructure. Other organizations, for example, manufacturers of machinery and industrial products utilize different industrial processes and these could be described as "non-critical", however, it is essential that all companies are alert to the potential risks to their ICS given the high profile fallout from industrial cyber-attacks. As risks continue to emerge in the field of ICS cybersecurity, knowledge of those risks are still growing and businesses need to keep up-to-date on the latest threats. Furthermore, it is interesting to take a look at the attitude of organizations with non-critical infrastructure towards ICS security. They are not as heavily regulated as companies with officially "critical" infrastructures and they have more independence on the decisions related to how to protect, or not to protect, their industrial network.

Industrial cyber security threats are all around and they come in many guises. These threats can be as simple as an industrial floor worker using an industrial PC for personal purposes such as Internet browsing. This simple act can have an impact on the control system which in turn can lead to the shutdown of manufacturing processes. In some instances these threats can also be highly sophisticated, planned and targeted attacks, designed specifically to jump over specific airgap and access the industrial network.

During the writing of this report in May 2017, the WannaCry ransomware attack has affected more than 200,000 systems in 150 countries around the world. Although the WannaCry malware was not explicitly designed to target industrial control systems, it managed to infiltrate ICS networks and can in some instance lead to the downtime of industrial processes. Among the industrial businesses affected were the Romanian car manufacturer Dacia, owned by France's Renault, which led to Renault temporarily stopping production at several sites to prevent the spread of the cyber-attack; the global car manufacturer Nissan, also reported that its UK manufacturing plant had been attacked but no major impact on its business was reported.

As industrial cyber-attacks become more widespread and global in nature, it's essential that industrial organizations identify and assess risks, and put in place the necessary policies, procedures and staff training to manage these risks thus reduce the likely impacts that any breaches may have on their organization.

Against this background, Kaspersky Lab, working with market research consultancy Business Advantage, conducted an independent research study of ICS/OT cybersecurity professionals in order to understand their attitudes to these topics and to identify the most important issues affecting their organizations.

In total, 359 interviews took place in 21 countries across the world. Of the companies interviewed, 56% were manufacturers, 19% were in construction and engineering and 11% in oil and gas. The remaining 14% comprised of utilities and energy, government or public sector, real estate, hospitality and leisure and defense. Additionally, 11 qualitative or in depth interviews took place and these included manufacturing and oil and gas companies as well as consultants and experts in the ICS cybersecurity field.

This independent research has found that industrial cyber-risks and cybersecurity issues in an ICS environment and happen on a constant basis. Over half of the sample of companies interviewed have experienced at least one incident in the last 12 months. The reported financial cost to business is also significant – the average annual cumulative loss was $347,603. In fact larger companies with 500+ employees, report annual cumulative losses of $497,097. The majority of these larger companies (71%) reported that they have experienced between 2 and 5 cybersecurity incidents in the last 12 months.

In general ICS security professionals are aware of cybersecurity threats to ICS in their industries, but they don't always have a good understanding of the specific dangers or do not have clear plans on how to deal with these issues. This was clearly demonstrated in the interviews that were carried out, where many different answers were collected on this issue. Three in four companies expect an incident to happen to their ICS, with larger companies feeling more at risk. Furthermore, the risk structure differs across the various industries and to different degrees of criticality.

Although most organizations (83%) feel prepared to manage those risks, they may be misguided in their preparedness as the current overall approach to ICS cybersecurity is a little chaotic. While some companies state they have security solutions set up, these are unlikely to be effective across many businesses unless the specialized solutions are deployed and robust processes and clear guidance is in place.

Add to this that there is little compulsory reporting of incidents – just one in five businesses were required to report breaches – and it is clear that incidents could be underreported. However, it is important to note that a significant proportion of the respondents have "non-critical" infrastructures or non-Government environments and this may explain their relatively more relaxed attitude towards reporting. Here we see an opportunity for regulatory bodies, such as CERT, ISAC and ISO, as well as governments, to play a positive role in helping industrial organizations with" non-critical" infrastructures to address the risks and bring about more transparency in reporting incidents.

However, companies must crawl before they can walk, and they need to start with their workforce to raise industrial cybersecurity awareness across their organization. This involves the training of ICS cyber security specialists (wherever they fit within specific organizations – IT team, OT, engineering, etc.) and raising the level of awareness of general industrial cybersecurity and safety through all levels of the industrial workforce. But because of the shortage of industrial cybersecurity professionals in the market, organizations may outsource specialized training needs where this expertise does not currently exist.

The report provides an overview of the industrial cybersecurity issues or risks facing organizations that run ICS environments and provides information to help those professionals tasked with managing these risks to compare their industrial cybersecurity preparedness with their peers globally.

This research will be conducted on an annual basis to monitor trends and changes in ICS organizational approach to face the challenges of industrial cybersecurity.

METHODOLOGY AND PARTICIPANT DEMOGRAPHICS

A total of 359 quantitative online surveys and 11 qualitative in-depth telephone interviews were conducted with ICS cybersecurity practitioners and consultants, including system integrators or IT consultancy firms. The research was conducted across 21 countries worldwide in early 2017.

The sample comprised a mixture of executive management (35%) and IT professionals (33%) across various industry sectors, particularly Manufacturing (56%), Construction and Engineering (19%) and Oil & Gas (11%).

Two thirds of the sample were in medium-sized organizations (100-4,999 employees), with one in 10 larger companies (5,000+ employees).

All participants were recruited as having some responsibility for making decisions regarding ICS cybersecurity and half of those interviewed held ultimate responsibility. Alongside their decision making remit, participant roles combined a number of responsibilities around ICS cybersecurity, including managing relations with external providers, managing ICS security budgets, communicating cybersecurity risks to executive management, as well as designing, implementing and managing ICS security relations.

RISKS, REALITIES AND PREPAREDNESS FOR ATTACKS

Industrial cyber risks are real

Cybersecurity experts consistently say that industrial environments are not protected well enough. Based on their experience and unbiased view, they say that often companies underestimate the impact of cyber risks and only build and invest in real security measures after a breach has happened.

Companies typically expect incidents resulting from vulnerabilities within external partners infrastructure and other third party system networks, and so are not prepared well enough for potential threats coming from within their partner organizations networks.

SPOTLIGHT: Chemicals Manufacturing

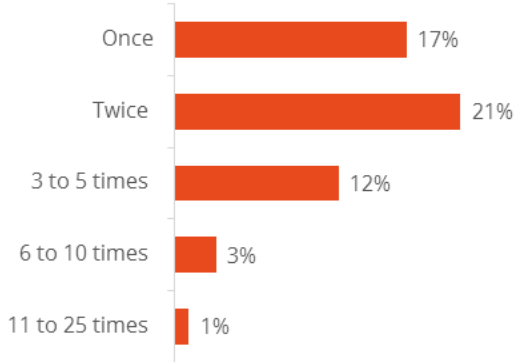
"We don't have any breaches on the industrial side as far as we know. I know we can never be 100% sure, but it is more antiquated equipment than cyber threat [causing problems] and we do monitor downtime."

Head of IT, Chemicals Manufacturing, UK

The reality is that organizations may not always know if there has been an attack on their control systems, either because the attack has been so subtle and designed to identify small weaknesses, or because the existing risk controls have successfully intercepted the threat.

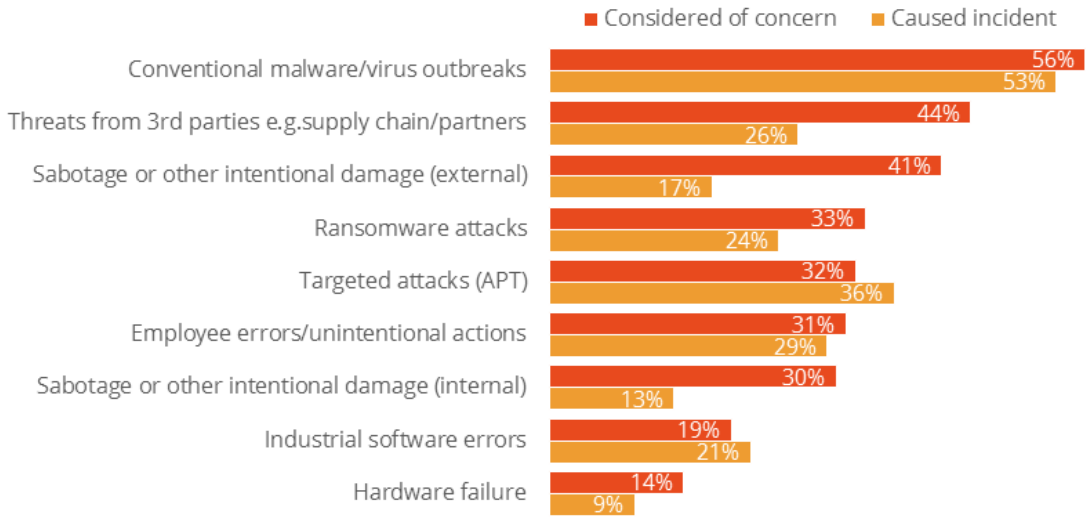
However, the threat of a cyber incident inside industrial control systems is real. Over half (54%) of the sampled organizations have experienced at least one incident on their industrial control systems in the last 12 months, with just over one in five (21%) experiencing two incidents in the same time frame.

54% of companies experienced an ICS security incident in the past 12 months



Concern outweighs actual incidence of attacks in most instances, suggesting a mismatch between the actual and perceived causes of ICS security breaches.

Perceived and Actual ICS Cybersecurity Threats



The majority of actual incidents (53%) were caused by conventional malware and virus outbreaks, which was also the main concern for the organizations interviewed.

From the research it is clear that targeted attacks, are perceived to range from casual malware infections such as spear phishing to more sophisticated Advanced Persistent Threats (APTs). Targeted attacks were in fact the second biggest actual threat to systems and caused incidents in over a third (36%) of companies. Surprisingly however, they were rated as only the fifth biggest concern. While human error was the third biggest reason for all incidents (29%), it was rated as the sixth biggest concern indicating a gap in perceptions.

The data shows that the number of targeted attacks is high and highlights that organizations must not underestimate the threat of security problems within their own business, particularly as this may arise simply by someone inserting a USB stick into an industrial PC and infecting control systems.

Of interest, the perceived threat from third parties was the second industry concern, followed

SPOTLIGHT: Goods Manufacturing

"Internal threats are more dangerous. We are well protected against external threats, but what is done internally has a direct path without a firewall in between. The threat originates unknowingly from members of staff."

IT Coordinator, Primary Goods Manufacturing, Germany

by sabotage or intentional damage by external factors in third place, and ransomware attacks in fourth.

The impact of a security breach is significant

The loss of product service quality and loss of proprietary information are the most likely consequences of an ICS security incident. But the consequences of cybersecurity breaches are far greater than simply financial cost. Companies seem to underestimate the impact on the environment and national security, but also the fact that – in their extreme – such incidents can result in loss of life, the reputational issues of which can significantly damage brands, lead to mistrust in industries and cause companies to close.

The cost to business is considerable

The average annual cumulative reported financial loss for a business affected by an ICS cybersecurity breach was $347,603 including the actual consequences of the incident and costs for software upgrades, staff and training.

The impact on larger companies is even greater. The annual cumulative losses for companies with 500+ employees is reported to be $497,097. The majority of these larger companies (71%) have experienced between 2 and 5 cybersecurity incidents in the last 12 months.

Companies are right to be concerned about ransomware attacks in particular.

SPOTLIGHT: ONGC India

"The cost of an attack can be enormous. Loss of human life, loss of natural resources are just some aspects, the actual cost can be very, very high. There will be fines and penalties as well imposed on the company as per the guidelines of the government."

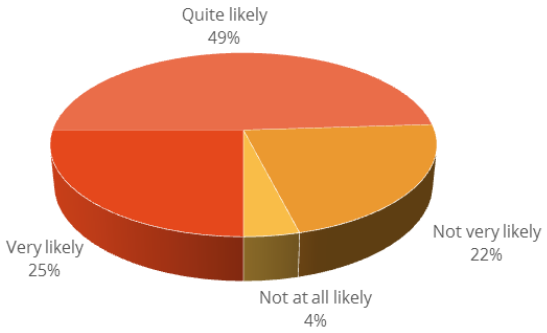
V. Suresh, Chief Engineer – Instrumentation, Oil and Natural Gas Commission of India (ONGC)

These caused a quarter of all breaches to industrial environments in the past 12 months and led to high financial losses. Businesses spent an average $381,529 dealing with the consequences and recovery from such attacks.

Awareness of potential attacks is high

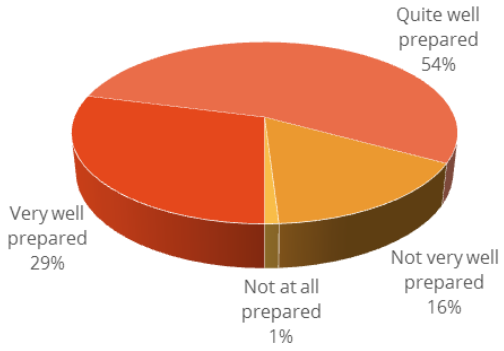
Three in four companies (74%) expect an ICS cybersecurity attack to happen to them.

Likelihood of an ICS Cybersecurity Attack



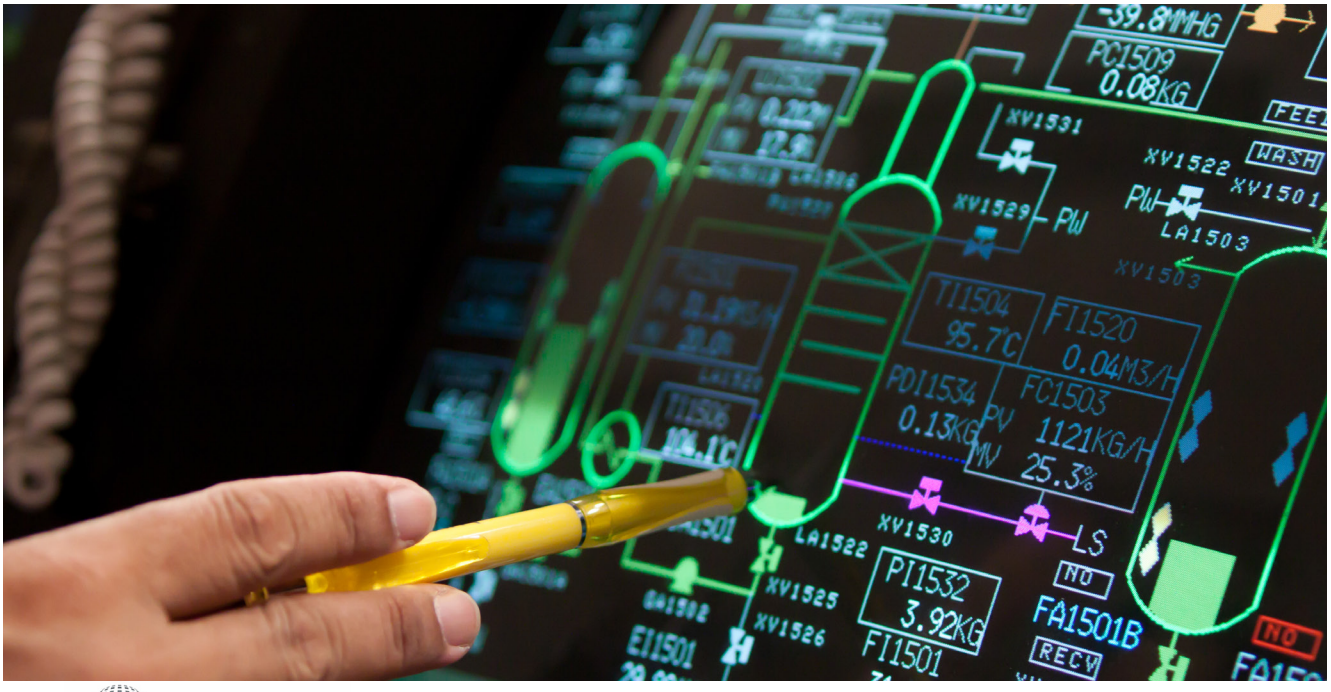
The majority of businesses (83%) feel quite prepared to combat such an incident inside their ICS environment: 86% claimed that they have an approved and documented industrial cybersecurity policy or program in place, which – critically – is approved by several departments within the company, including executive management (41%), IT (41%) and IT security (42%).

Readiness for an ICS Cybersecurity Attack



However, there is an indication that organizations are not yet fully prepared, with comments made that staff are not as aware of the threat of cybersecurity infractions as they should be.

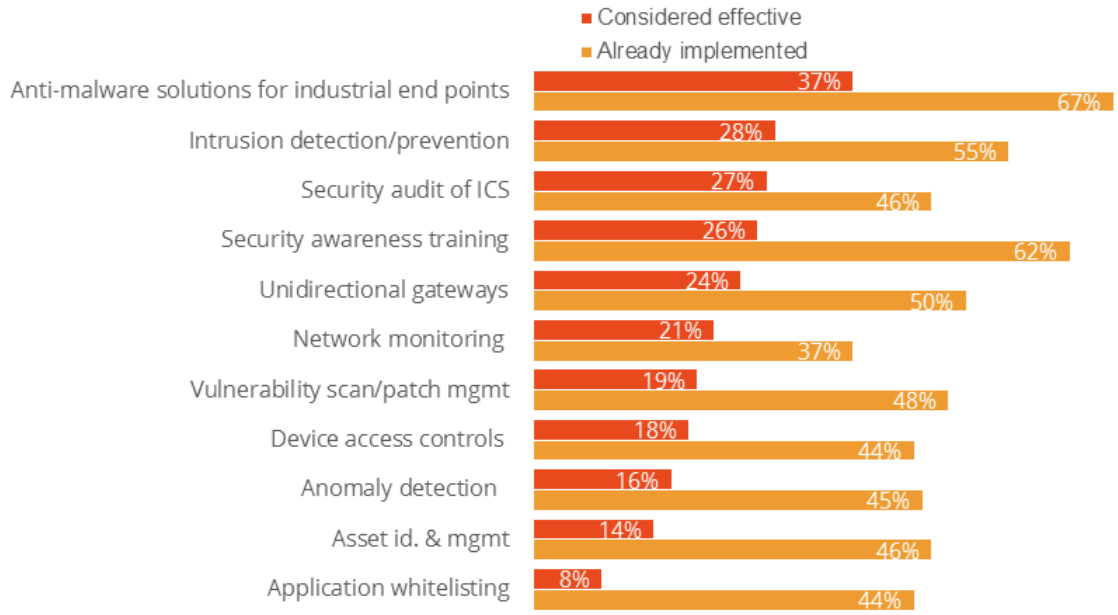
There is a clear opportunity and need for organizations to test their procedures and better understand how to identify potential weaknesses and risks around ICS security. Fixing these problems now and introducing regular testing designed to identify and minimize vulnerabilities will help to prevent future incidents.



IMPLEMENTING EFFECTIVE MEASURES TO MANAGE RISKS

Most companies seem to have a good idea of the potential effective measures needed to combat ICS cybersecurity breaches. However, given that 55% of organizations experienced an incident in the last year, it can be assumed that the measures adopted were either not sufficiently robust or there was something wrong with their implementation. This could have included using a solution not designed for an ICS environment, not having the right settings and controls in place, or simply that the measures were not working (for example, anti-malware was erroneously switched off).

Perceived Effectiveness and Implementation of ICS Security Measures



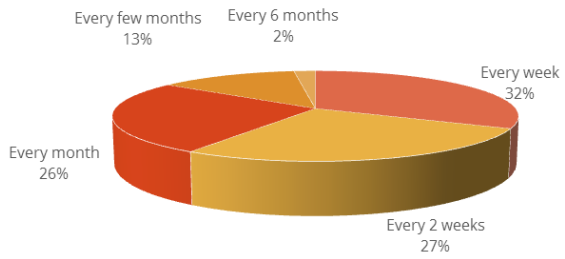
Organizations considered anti-malware solutions as the most effective measures to combat ICS cybersecurity breaches for an industrial setting, and were in use by just over two thirds of companies. A similar proportion (62%) had implemented specific security awareness training for their staff, and had increased their control over remote and wireless access to their networks.

However, the efficacy of application whitelisting is doubted as it was considered effective by just 8% of the 44% of organizations which had implemented it.

Among the measures with lower current usage, there is most short-term interest in implementing tools for detecting industrial anomalies and unidirectional gateways between control systems and the rest of the network, as well as IPS/IDS systems.

There is also scope for companies to further protect themselves with increased usage of vulnerability scans and patch management. As the WannaCry pandemic has shown once again, the up to date patching of generic systems like Windows OS is a crucial security measure. Currently these are run regularly (at least fortnightly) by six in ten of the sample, with the remainder taking this action more infrequently.

Frequency of Issuing Patches/Updates



For 55% of companies that said external parties, such as partners or service providers, can access their industrial control network, third party policies should be in place aimed at reducing potential risks to the control system. The data proves that organizations allowing third party access were 63% more likely to experience a cybersecurity breach, compared to 37% of those who did not.

In addition, there are indications that many companies have larger attack surfaces, by using wireless connections on their industrial network (eight in 10). This highlights a need for education and assistance to ensure the network security of industrial environments and to reduce the risk of any kind of breach.

SPOTLIGHT: HKA Global

"It is growing [wireless network used often for industrial control equipment]. There is a lot happening around IoT - control systems side of things like buses and autonomous vehicles, that is all going to be wireless. Where you have machines ordering their own replacement parts or other maintenance parts, you are bridging the gap between manufacturing and IoT and that is going to have a huge implication for security measures."

Lars Janowski, Director and Head of Transformation, Innovation & Technology Advisory, HKA Global, Australia

SCADA as-a-Service

The vast majority of companies appreciated the benefits of Supervisory control and data acquisition SCADA-as-a-Service – 38% of our respondents already use cloud-based SCADA and 40% plan to introduce it in the next 12 months. While organizations appreciated that this would take time to implement and embed, just 5% have no interest in implementing this or any other cloud-based control solution. The usage of SCADA-as-a-Service over wireless connections means that companies need to take a more thoughtful approach to the security model of the industrial organization.

Although SCADA as-a-Service is not widely spread yet, the level of adoption is expected to grow in the near future.

Siemens and SAP recently announced a joint effort in the field of SCADA as-a-service. When asked if he thought such bigger players would help to speed up the adoption long term, Mr Janowski said:

"Yes, not just long term, more medium term I think, almost certainly. If you think about the clients who are the larger organizations: they have the on-site engineers and long term contracts with suppliers and they have the licenses and all this. It will slow down at some point and they will see the advantages of using things 'as a service' in the same way IT saw the advantages and adopted SaaS and as licenses were running out they tried to put it out in the cloud because they don't need certain features, so they just take what they need. I think it is a natural progression as part of the future."

SPOTLIGHT: HKA Global

"I think it is certainly picking up. Less for clients in Oil and Gas, for example, who by their very nature are very remote, so they may be in the middle of the desert for some of their work. It is difficult to get a proper connection, which is topped off by Australia not really having the highest internet speed across the country. That is a major problem, meaning it would help if the internet was better and faster. That is one of the reasons [for slowing adoption of SCADA as-a-service]."

Lars Janowski, Director and Head of Transformation, Innovation & Technology Advisory, HKA Global, Australia

REDUCING RISK, PROTECTING SYSTEMS AND REPORTING

Based on in depth interviews with IT professionals in ICS environments, ICS cybersecurity risk management is recognized to be a growing need for organizations. It is therefore important that companies know what the potential risks are. They also need to have trained and qualified staff available to identify these risks and manage the business's response, and also have in place the right controls and software to protect those systems and hardware.

There is a clear need for raising levels of awareness of all staff about the cyber risks within operational technologies. Furthermore there is a need to have access to dedicated industrial cybersecurity specialist staff internally to educate the wider workforce.

When asked if ICS cybersecurity gets enough attention within their organization, one respondent from a UK tools manufacturing company said:

SPOTLIGHT: Machine Tools Manufacturing

"No, certainly not at the moment. The discussions on this topic are in their infancy. We are discussing it within our own business and with the trade associations as well.

The feeling I get from a number of

Contd...

other companies is that they are also at discussion stage. It's been around for some time, it is not new. I think maybe in the past, some of the larger organizations have been tapping into or exploring this kind of technology. But for smaller businesses and SMEs, I think cost has been one of the drivers and also just the lack of knowledge in terms of how and what actually it can do for you has been a factor as well."

Technical Director, Machine Tools Manufacturing, UK

Companies are struggling to find the right staff and external support to help them to manage and reduce the industrial cyber risks. For 50%, finding employees with the right skills to manage ICS cybersecurity is a priority, and a main priority for 15% of those businesses. Finding reliable partners able to implement solutions is a struggle for 48% of businesses, with 13% listing it is a main priority

SPOTLIGHT: ONGC, India

"Getting the right people and updating their knowledge are the biggest challenges. As industrial cybersecurity is a very dynamic field, a lot of training is required".

V. Suresh, Chief Engineer – Instrumentation, Oil and Natural Gas Commission of India (ONGC)

Challenges of Managing ICS Cybersecurity

SPOTLIGHT: Inycom, Spain

"There is a lack of awareness among the workers – we need to raise security awareness, we can implement this measure with cyber games, gamification, courses - to teach workers about potential threats to a plant, or we can provide a specific course about cyber security to the responsible plant manager."

Aitor Lejarzegi Zabala, Industrial IT - IACS & IIoT Network Security, Inycom, Spain

SPOTLIGHT: HKA Global, Australia

"Understanding what the impact [of a breach or attack] can be and if you have a risk management framework in place that will enable your people to understand what would happen, what would be the mitigation plans if something happens and who are the responsible people for that and raising the awareness of that is a huge factor. That already can make about 50% of the problems go away. If you take the technical measures on top of that, I would say you are pretty safe."

Lars Janowski, Director and Head of Transformation, Innovation & Technology Advisory at HKA Global, Australia

An opportunity for governments and regulators to improve industry reporting

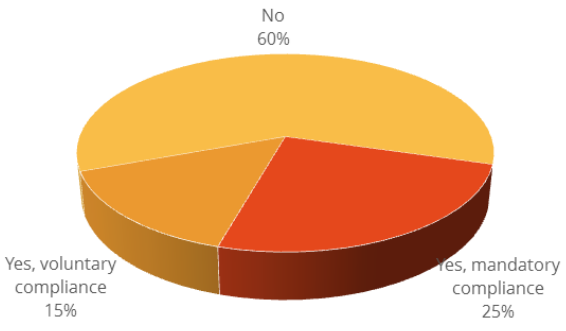
Organizations that have critical infrastructure such as those in oil and gas transportation are already heavily-regulated and have strict reporting procedures in place. However, there is a clear need for more government and industry guidelines and reporting standards to be developed for "non-critical" industrial organizations, including for example machinery manufacturers. In the company sample (most of which were manufacturers), just one in five industrial businesses is required to report any cybersecurity breaches, yet two thirds of businesses would welcome such a move.

SPOTLIGHT: Inycom, Spain

"It is curious to watch all the hype around the forthcoming EU General Data Protection Regulation. Protection of personal data is very important, but what about protection of data that defines industrial processes and the protection of processes? At the end of the day, the aftermath of compromising the industrial process is potentially much more dangerous in comparison to compromising personal data. I would like to see the creation of a powerful European or global regulation for industrial cybersecurity, which would be similar to GDPR."

Aitor Lejarzegi Zabala, Industrial IT - IACS & IIoT Network Security, Inycom, Spain

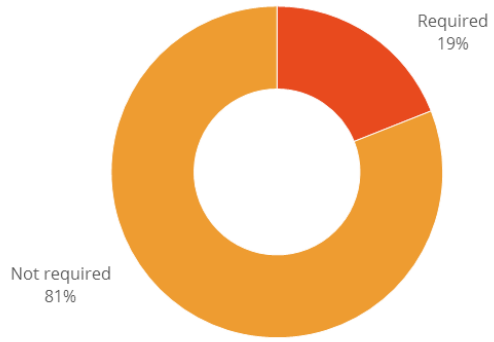
Compliance with Government Regulations



As there is limited compulsory reporting, there can be a tendency to withhold at least some incident reporting to protect brand reputation: 22% of businesses did not report any incidents at all, while a third had reported only some of the breaches.

The highly publicized consequences of the international WannaCry ransomware attack in May 2017 are likely to prompt an earlier discussion given the implications that future (or continued) risks could have on the industry in future.

ICS Security Breach Reporting



Reflecting the globally emerging nature of this field, on average globally there is limited guidance and regulation within the area of industrial cybersecurity, with just a quarter of companies stating that they have to comply with industry or government guidelines. Two thirds of businesses said they would welcome some level of compulsory reporting.

Improved transparency brought about through better guidelines and required reporting could help companies to build on internal procedures for managing incidents and raise overall awareness of the size of the problem given current underreporting.

RISK PROFILING AND EFFECTIVE PREVENTIVE MEASURES

Using our research findings, we have identified a risk profile for industrial businesses to assess their level of preparedness against a cybersecurity breach.

The measures outlined in the second and third examples below can be taken by any organization to improve the overall cyber risk management framework and to better secure the ICS.

SPOTLIGHT: Subsea Control Systems

"The company is focusing more on cybersecurity and I sometimes feel that this is becoming a headache when I have to create a balance between cybersecurity and production and operation, which delays matters. At the same time it is much needed for the security of the company and the data. From the company's point of view, it is good and needed but at the same time it is hampering productivity."

Senior Lead Engineer - Subsea Control Systems, Oil and Gas: Extraction and Processing, India

Risk factors of facing a cybersecurity breach:

Organizations that have typically:

- allowed access to external parties
- do not comply with any industry/government regulations around ICS cybersecurity
- use wireless connection for the industrial net work*

Better prepared for a cybersecurity breach:

Organizations that have typically:

- approved documented cybersecurity policies or programs in place
- implemented a range of security measures
- conducted security assessment/audit of ICS and control networks
- installed a unidirectional gateway between control systems and rest of network
- run vulnerability scans and issue patches every week or two

*statistically likely to be slightly more open to attack.

Best prepared to defend a cybersecurity breach:

The organizations that stated they have not experienced any incidents/breaches in the past 12 months have implemented the above measures and also:

- installed anti-malware solutions for industrial endpoints
- used industrial anomaly detection tools
- run intrusion detection and prevention tools
- provided staff and contractors with regular security awareness training.

CONCLUSION

Clearly, there is a great deal of work to be done to ensure that industrial companies are best protected as possible against the increasing risk of cyber security breaches in their ICS environments.

Industrial cyber incidents happen frequently – over half of the sample had experienced at least one incident in the last 12 months. But despite awareness of and claimed readiness for infractions, companies are often underestimating both the source and impact of such incidents. It's essential that steps are taken to identify the risks to ICS environments, with the rigorous policies and procedures put in place to manage those risks so that the company is in the best possible position to secure its operational technology.

In addition to significant financial loss, the impact of an attack – whether intentional or not – can be considerable on a company's industrial process, products, proprietary information and reputation. In the worst cases, these can result in the loss of life, damage to the environment and the closure of a business.

Approaches taken to managing industrial cybersecurity are somewhat unstructured and could be improved. Despite many organizations stating that they have security solutions in place, their efficacy could be reached only if specialized ICS-aware security solutions are deployed and supported by robust processes and clear guidance. Against the backdrop of real threats to industrial control systems, relying upon a standard out-of-the-box security product would be akin to applying a "band-aid" to an injury affecting an artery.

It is also highly likely that incidents may be considerably underreported (specifically amongst non-critical infrastructures) with the true impact on the businesses a relative unknown as there is little compulsory reporting of ICS cyber breaches required (just 19% of businesses were required to report such breaches).

That said, two thirds of the sample welcomed a potential move to some level of mandatory reporting and governance in their area of business, creating a clear opportunity for regulatory bodies, such as CERT, ISAC and ISO and others, to help organizations bring about more transparency in reporting incidents and to help develop frameworks to address the risks. We see this as an open door, which would result in better reporting of, management of and protection against future cybersecurity infractions.

True cybersecurity starts with people – companies conducting security awareness programs for staff, contractors and partners typically experience less financial loss. Investing in cybersecurity awareness for all staff is critical in the 'war' against industrial cyber risks.

Industrial businesses based on operational technologies require people armed with the necessary skills and training to help provide specialized protection of that infrastructure.

That is why having skilled and trained ICS security professionals, who understands the needs of the two worlds of ICS and cybersecurity, is also extremely important for ant modern industrial organization.

Where such talent does not exist within an organization, it is essential that this critical resource is outsourced.

ABOUT KASPERSKY LAB

Kaspersky Lab is a global cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization –including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and the consistency of technological process.

Learn more at www.Kaspersky.com/ics

Business-Advantage.com