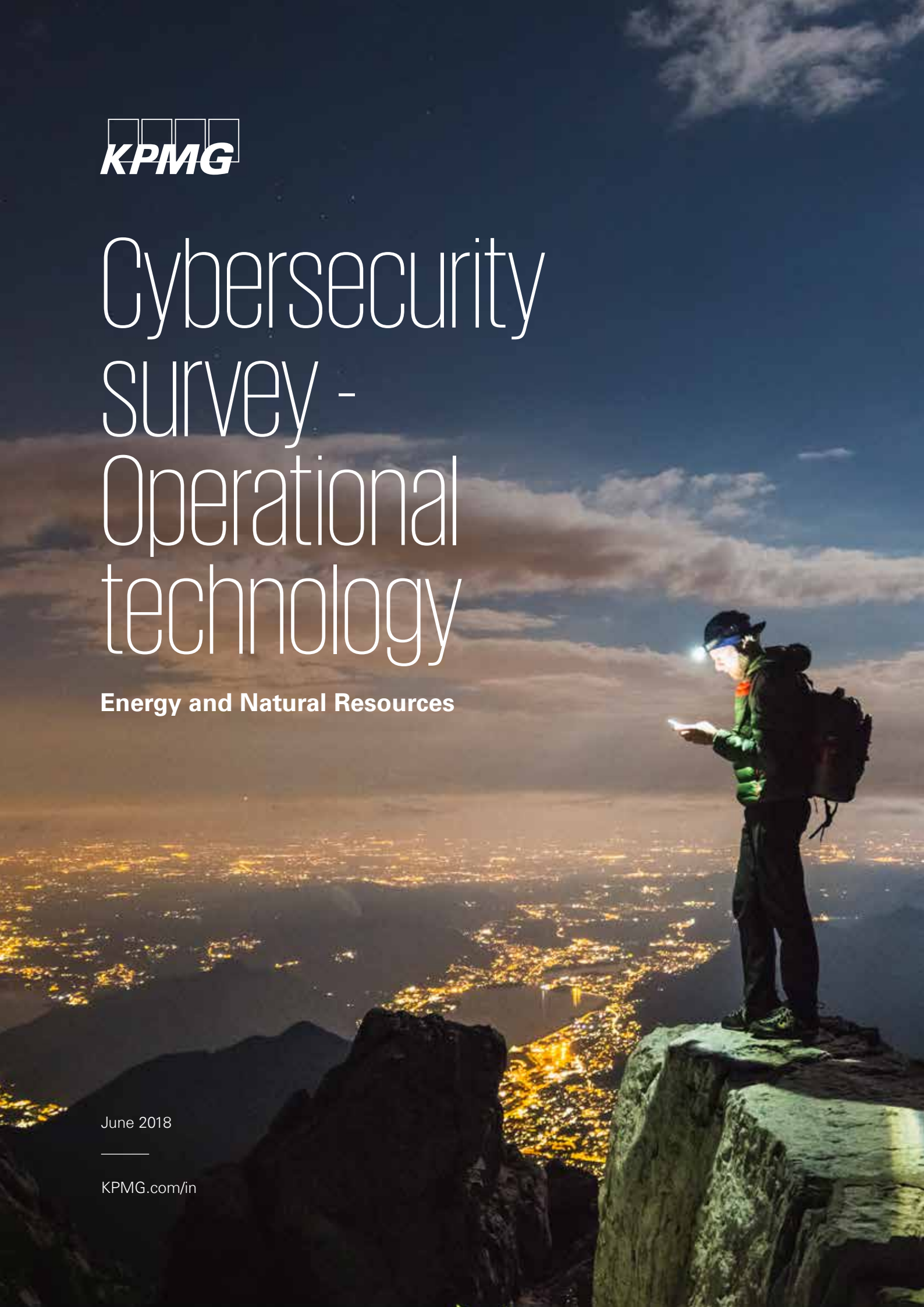


Cybersecurity survey - Operational technology

Energy and Natural Resources

June 2018

KPMG.com/in

TABLE OF CONTENTS

TABLE OF CONTENTS

Foreword

Cybersecurity is a strategic enterprise risk that goes far beyond Information Technology (IT). It is no longer just the focus of IT Team but has taken the place on boardroom agendas, as board members are increasingly concerned about protecting their companies' valuable assets and operational equipment which might be vulnerable to cyberattacks. It is absolutely imperative for organisations to sit-up and take notice of the present dynamic cyber environment and take preventive actions proactively.

The Energy and Natural Resources (ENR) sector is one of the most important sectors in the economy of any nation state. The impact of cyberattacks in this sector are wide-ranging for any organisation and may even have global political and economic ramifications in certain instances.

Paradigm shift in the nature of the Information Technology (IT) and Operational Technology (OT), behooves organisations to ensure an appropriate cybersecurity agenda is taken up and dealt with on a 'war footing' without losing focus. Given the proliferation of connected technologies, there would be huge impact of any cybersecurity breach in case a real-time OT system is compromised. Today, C-level executives are concerned about increased cybersecurity threats and about newer incidents that are being reported.

KPMG in India has been at the forefront in helping clients address cybersecurity requirements across industry verticals. This survey focusses specifically on the ENR sector and identifies some of the critical challenges faced by its OT environment.

This survey attempts to analyse the preparedness of organisations to deal with cybersecurity threats in the sector.

We hope the survey report provides insights that can be leveraged in shaping the cyber risk management posture of your organisation.

By reading this report, we hope the management and control system professionals in the ENR sector in India gain insights into the challenges faced by their peers, as well as boost their preparedness to reduce the risk of cyberattacks.

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader
Global Cyber Security

Anish De
Partner and Head
Oil and Gas

Atul Gupta
Partner and Head
IT Advisory
Risk Consulting
Cyber Security Leader

Highlights

Operation Technology in today's process control systems is opening several connections to the external networks and the internet, and are being administered over handheld mobile devices owned by system administrators. Due to the huge impact, it has become imperative to bring the OT systems within the purview of cybersecurity and make them secure. Historically, IT and OT were maintained and managed separately. IT was traditionally associated with back-office business systems such as accounting, billing and customer records. OT was traditionally associated with field devices and the systems to monitor and control them such as supervisory control and data acquisition systems (SCADA) and distributed control systems (DCS). However, the companies in the ENR sector are now deploying advanced automation for significant bottom-line improvements in the integration of IT and OT systems, which has made these companies vulnerable to increasingly frequent cyberattacks.

Building a secure and a reliable defense mechanism against all types of cybersecurity threats has proved to be a challenge especially because different domains are typically administered with the help of silos / segregated departments. The task is made all the more difficult by the diffused nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

The U.S. ICS-CERT responded to 290 reported cyber incidents against control systems in fiscal year 2016. The Critical Manufacturing Sector accounted for 63 of these incidents, while the Communications Sector had 62 and the Energy Sector had 59. Of those incidents, 26 per cent were the results of a targeted industrial control system (ICS) spear-phishing campaign, which makes it one of the leading attack vectors used by cyber criminals. Network scanning and probing accounted for another 12 per cent. With confidential strategic data, operational information at stake and reputations on the line, organisations in India are also now beginning to realise the immediate need to build strong and robust cyber defenses. As boards across organisations work on understanding the various dimensions of cybersecurity in the energy sector, it is also important to understand that investing in cybersecurity is the need of the hour and is perhaps the one of the way to help ensure stable business operations against the menace of cybercrimes.

Source: ICS-CERT Year in Review 2016

OT – the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.

To find out how organisations are dealing with the risk, KPMG in India conducted an in-depth survey of the prominent ENR companies in India to determine their risk awareness and security practices. Our survey report provides the view of Indian corporates in the energy sector which is summarised below:

Only **27** per cent have a well-defined cybersecurity policy for OT setup supported by OT security team.

However **71** per cent rely on reports provided by external auditors and SMEs (either directly or via OEMs) for determining the security posture of their OT.

For **31** per cent OT systems are not being adequately patched.

Further **39** per cent are of the opinion that OEM should replace the systems with more secure systems to continue being in business.

Nearly **38** per cent are of the opinion that the OT support team has limited skills on security posing a major risk to the OT environment security.

31 per cent are neither associated nor aware of sectoral CERT, National Critical Information Infrastructure Protection Centre (NCIIPC) initiatives.

Across **54** per cent management believes that a centralised robust policy should be formulated covering the critical infrastructure sector.

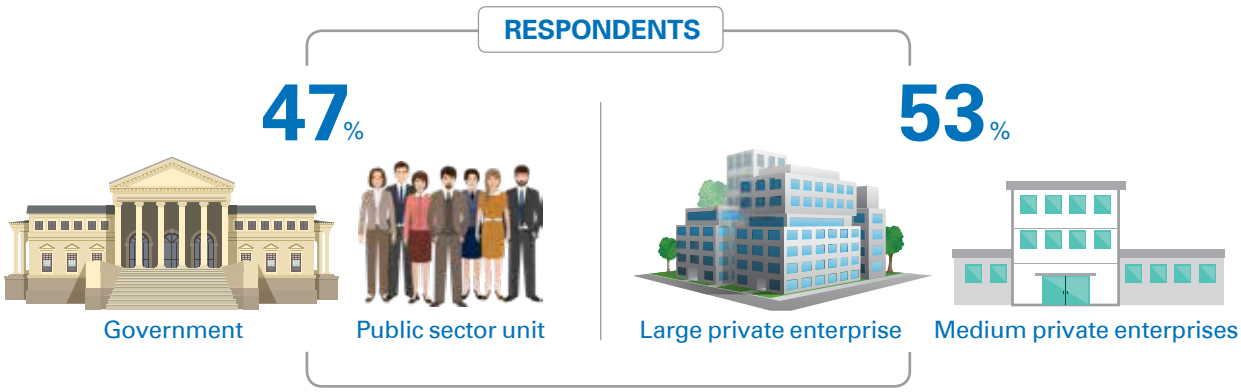
Nearly **31** per cent are of the opinion that support is required in collaboration and knowledge sharing on cyber incident between critical infrastructure industries to improve the cybersecurity posture in the OT environment.

Introduction

The survey aims to provide the ENR industry with a reference point about the key aspects of cybersecurity in OT environment. The survey sheds light on aspects like responsibility and ownership of OT security, policy making, and risk management in OT environment, security training and awareness methods, dependence on OEM support for cybersecurity and the related contractual binding and also the expectations from sectoral CERT for advisory and actionable in cybersecurity.

KPMG in India has carried out this cybersecurity survey across a wide range of companies operating in the ENR sector within India.

Respondents represented a variety of organisational sizes, types, locations in India. About a half of them were from the public sector and government organisations, and the rest from large and medium private enterprises.



Source: KPMG in India's operational technology survey 2017-2018

All the respondents are responsible for OT, system administrators supporting OT systems, OT security team or management representatives who are directly responsible to ensure the reliability and security of control system environment.

Prioritising the OT security framework

One of the first tasks that an organisation needs to do to secure its OT environment is to define and setup a cybersecurity policy covering the OT environment. It is obvious that without rules, responsibilities, formal procedures and their awareness amongst users / process engineers, a cybersecurity framework can never be effective. It is the first step towards aligning information technology with business objectives.

An effective set of policies and processes can go a long way in ensuring that a consistent approach is followed for securing OT systems and that these systems are protected from various internal and external threats on strategic infrastructure.

Despite an essential first step,

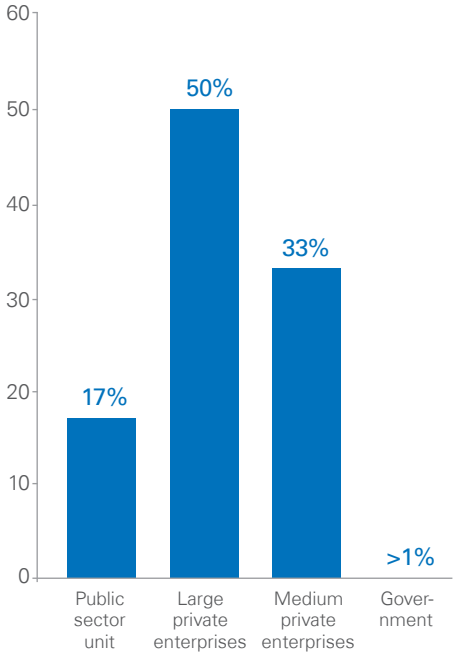
33 per cent

of respondents have revealed that they are yet to define any policy and processes related to OT security and another

40 per cent

of the organisations have decided to use a mix and match approach whereby aspects of OT security are covered as part of the overall security policy and are supported by the IT cybersecurity team of the organisation.

Organisations which adopted OT Policy from IT policy



Source: KPMG in India's operational technology survey 2017-2018

At a minimum, an OT cybersecurity policy needs to include the following:

01 OT cyber security objectives

02 Risk Management Frameowrk

03 Compliance requirements

04 Asset management

05 Continuous monitoring

Responsibility of framework implementation

It is not enough to simply define the policies, and its equally important to implement the policies. Similarly, establishing an Operation Technology Security Group (OTSG) to implement the policies and to supplement the cybersecurity team's efforts would be required to defend against directed attacks. OTSG groups have initiated basic steps in that direction and started to setup teams to specifically focus on the requirements in this area. However, many organisations have not initiated any steps towards securing their OT environment.

The key reasons driving these changes at various organisations are:

01 Difficulty in managing OT environment due to inherent complexities involved without a focused team

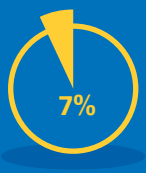
02 Increased threats and the complexity of cyberattacks on environments

03 Perception of OT in the ENR sector being especially targeted due to the strategic importance of this sector for a nation.

Source: KPMG in India's operational technology survey 2017-2018

Organisations have assigned the responsibility for securing their OT setup to their Operations teams

Organisations have identified and dedicated a person to manage the security of their OT setup



Organisations identified OT security as part of overall corporate cybersecurity team which is responsible for taking all the strategic decisions

Source: KPMG in India's operational technology survey 2017-2018

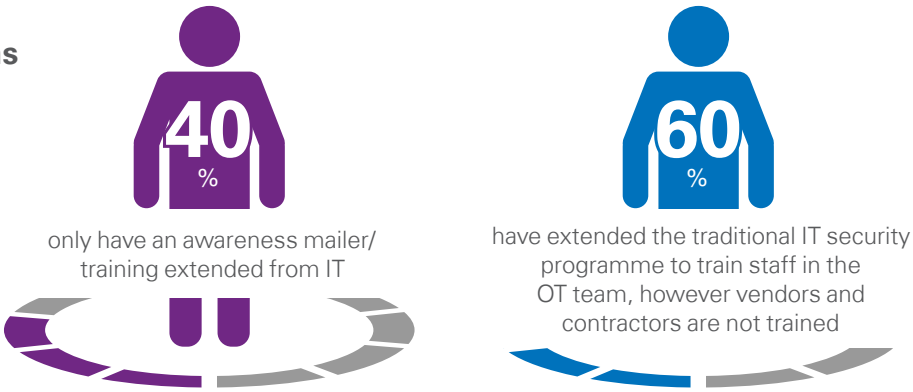
Cybersecurity awareness

Training and awareness is key for a secure OT environment. Even with the best technology in place, one of the weakest links in an organisation, for cybersecurity, is its employees.

The prevalence of the vanishing perimeter holds an even greater emphasis on proper cyber hygiene, which can be taught by a good security training programme. The teams in any organisation have to stay on top of the latest cyber threats out there that look to exploit the human element, especially cybersecurity threats emerging from social engineering attacks and this can be achieved through effective training programmes, regular testing and periodic drills.

What stood out was that none of the organisations have a well-defined cybersecurity programme focused on OT, to measure its effectiveness through mock drills. Despite all the respondents agreeing that there is an absence of a focused OT security programme, all of them have taken initiatives towards security awareness training for staff, contractors and vendors.

All of the organisations surveyed have taken some or the other initiatives towards security awareness trainings for staff, contractors and vendors.



Source: KPMG in India's operational technology survey 2017-2018

Managing cyber risks

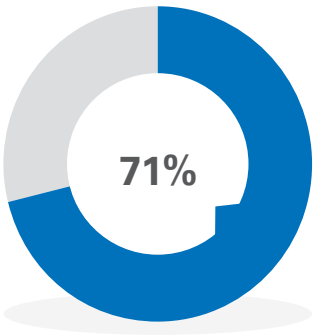
Managing cyber risks

Risk Management is an iterative process of risk identification & assessment, controlling, and mitigation. The key to having resilient operations is to have an effective risk management strategy which is focused on the OT landscape.

Organisations today need to establish a technology risk management framework to manage operations technology risks in a systematic and consistent manner very similar to the one IT has adopted for enterprise IT network. This can be achieved by the assessment of the impact and likelihood of current and emerging threats, risks and vulnerabilities and having effectively designed robust controls in place as well as allocating roles and responsibilities and the identification of cyber assets in the control system environment.

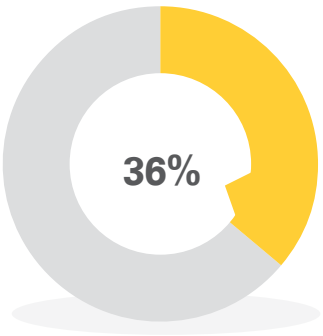
Risk assessment

The risk assessment approach should be proactive. The approach adopted by most organisations in ENR sector in India identifies a significant role for external auditors or OEM, since the people with the required skillsets and experience are in short supply and very few companies have them on board.



of the survey respondents depend on external auditors to assess the risk in their OT environment and to provide recommendations to remediate the gaps identified.

of the respondents trust their OEMs to engage with external auditors and SMEs / consultants to assess the risks and carry out mitigation steps.

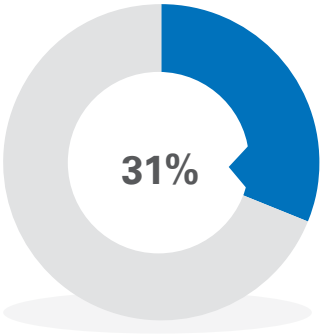


of the respondents are yet to carry out any type of audit (internal or external) of their OT environment to assess the risks. This means many organisations are still working with obsolete information / systems and are prone to cyberattacks.

Source: KPMG in India's operational technology survey 2017-2018

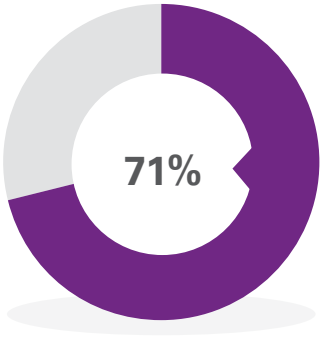
System security patches

Installation of vendor supplied patches on a regular basis is the most common and primary method used by respondents to ensure the security of OT cyber assets. However, only



disclosed that OT systems are not being adequately patched.

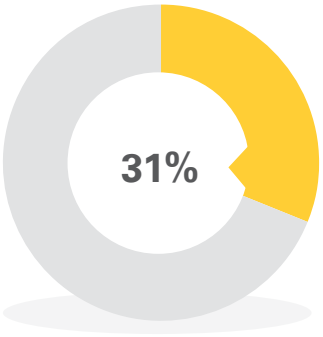
Outdated patches are the most common vulnerability which are exploited by internal or external cyber criminals. A minimal patch management programme must at least provide security practitioners an awareness of the software and systems which are out of date so they can monitor and protect against any relevant exploits. Further,



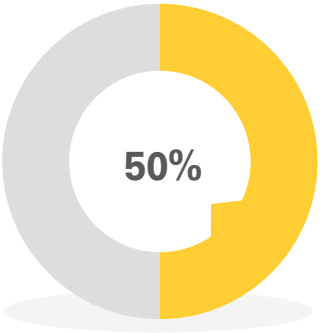
respondents claim that their organisations' internal operation team manages the patch deployment for all the devices, workstations and servers deployed in the OT network.

Source: KPMG in India's operational technology survey 2017-2018

Secure remote access



of respondents have responded that managing cyber risks is becoming difficult due to the deployment of control system assets at remote locations. Another factor mentioned was the requirement to provide remote access for vendor support or SCADA monitoring nodes and other data servers.



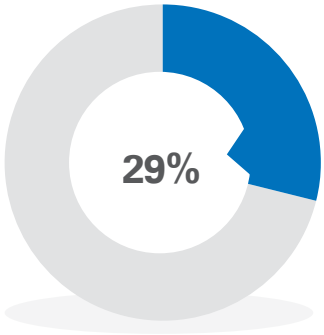
organisation provide access to their OEMs for logging-in and providing support to OT teams through Untangle VPN

Support from OEMs in the implementation of controls

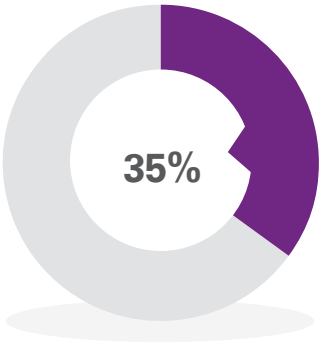
While organisations work towards comprehending the complexities and strengthening their policies and processes to ensure higher level of security, the role of OEMs in assisting organisations in controlling risks towards the OT is quite significant. Respondents to the survey depend on their OEMs in order to:

- Obtain security advisories to act upon
- Provide limited / full support to keep their systems / devices secure
- Perform support tasks for the OT environment by logging-in and securing the systems.

None of the surveyed organisations rely on the tools / applications and processes deployed internally (even when they claimed to be self-sufficient) to identify the risks and perform corrective actions independently without OEM involvement.



of the surveyed organisations rely on OEMs to identify and monitor the attacks / intrusions.

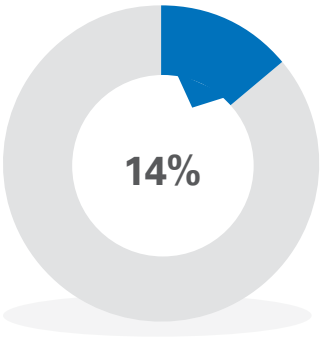


of the respondent organisations receive advisories from OEMs.

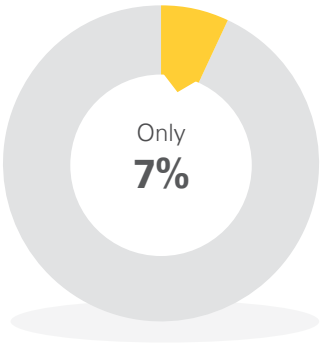
Convergence of the IT and OT network

IT and OT systems were traditionally kept separate, whereby IT systems dominated the networking and communications requirements while OT made use of basic programmable logic controllers and some proprietary protocols and systems to deliver. However, process control systems are opening multiple connections to external networks and internet and with the advent of IoT, increased automation requirements, and newer sensors – there is a blurring of the gap between the traditional operating domains of IT and OT. This has led to a perceptible increase in the IT and OT convergence and with it, an inherent increase in the attempts to maliciously attack OT systems.

OT and process control systems were never intended to be operated remotely and over the web, and therefore have little or no native security. As such, organisations have started to deal with the security requirements of OT systems separate from the IT systems and looking out for specific solutions and processes to strengthen the OT system security. Our survey findings indicate:



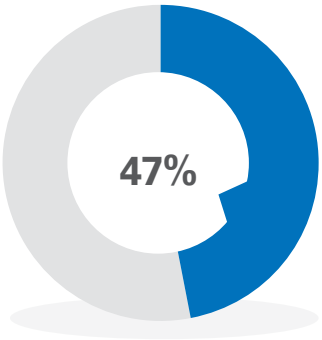
organisations disclosed that they have IT and OT equipment connected on same network with no network traffic screening / filtering.



organisations have separate setup for IT and OT network to have an air-gap between the two setups.

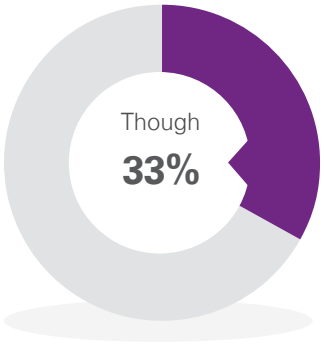
Implementing risk remediation measures

Organisations realise the strategic criticality of the OT in their overall business environment and have instituted a formal process to ensure that the cybersecurity risks identified in OT environment are appropriately dealt with. To that effect most organisations discuss the risks identified within the Central risk committees to gain a strategic view of the risk and potential options to deal with these risk. We observed that

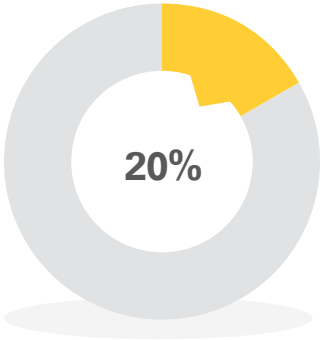


of the organisations which responded to our survey, report their cyber risks identified during assessment to central risk committee. However, some of the unique challenges identified by respondents in implementation of security controls in OT environment include:

- OT systems which were deployed long time back do not support risk remediation measures
- Lack of security technology solutions for control system environment which can reduce / mitigate the risks
- Cybersecurity awareness for OT system support team including engineers and operators is low which exposes environment to higher risks.

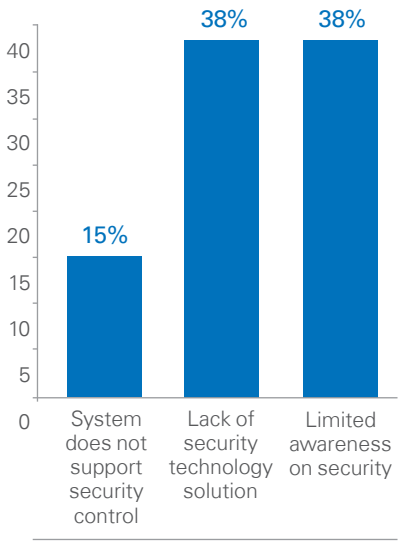


of organisations in our survey stated that they have identified a person who is responsible for OT security,

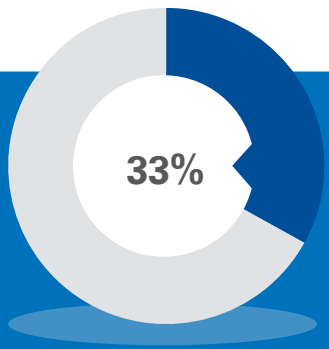


still have an ad-hoc process to manage the cyber risks.

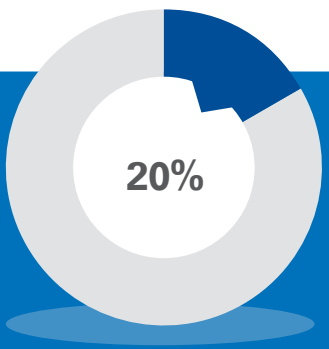
Constraints impacting security remediation measures



Source: KPMG in India's operational technology survey 2017-2018



of organisations stated that they have identified a person who is responsible for OT security

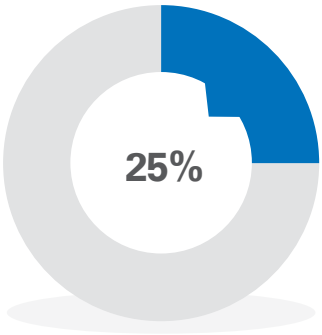


still have an ad-hoc process to manage cyber risks.

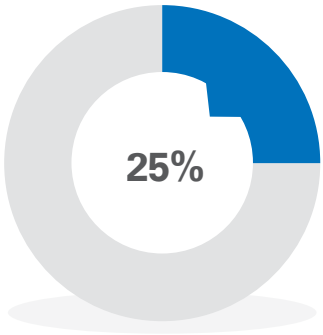
Security breaches: Handling incidents

Security incidents

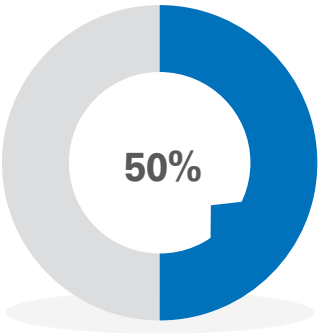
While being able to detect a cyber incident in a timely fashion is important, it is also important to handle such incidents effectively on the OT environment. It is imperative to have a well-designed response plan and ownership defined for damage control and recovery procedures. Hence, establishing an effective incident response programme is a key component of an OT risk management strategy.



organisations disclosed that they follow an ad-hoc way of responding to OT cyber incidents

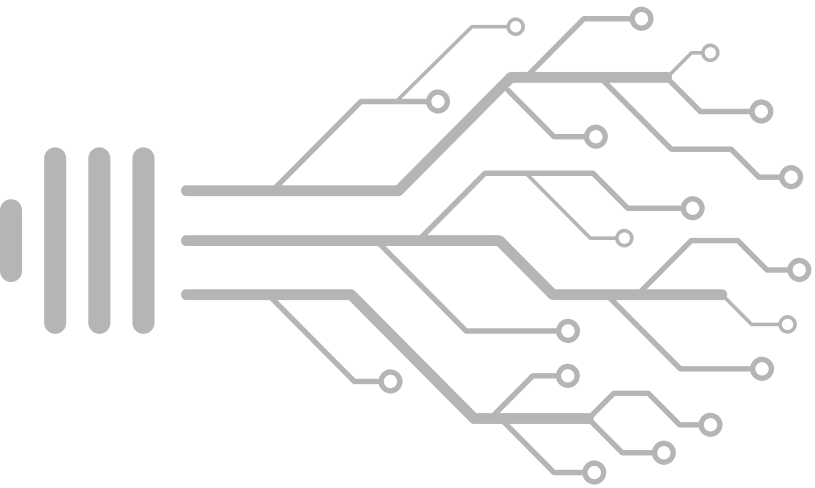


organisations have a formal process to responding, documenting and learnings on incidents



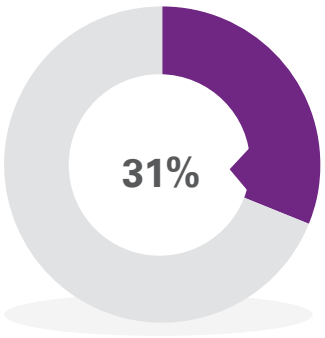
organisation have a robust process to deal with any security incidents. This process is not specific to IT and / or OT setup only

Source: KPMG in India's operational technology survey 2017-2018



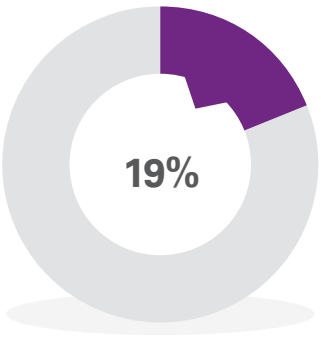
Contractual binding with OEMs

In today's scenario of a connected world with remote support the dependence on OT vendors for smooth operations and managing valuable and sensitive information is very high. This leads to an increased risk of the OT systems being compromised by malicious actors not only in organisation setup but also in extended enterprise. Having a liability clause on cybersecurity helps organisations to reduce the risks associated. Just like any other product or service which is expected from any supplier, adherence to the cybersecurity clause should be considered as a deliverable from the supplier.



organisations disclosed that their contracts with equipment providers are silent on the cybersecurity of provided equipment

organisations have contracts with OEM that binds them to keep a plug on the cybersecurity gaps and keep customers updated within defined timelines also it bind OEMs to provide only tested and certified OT systems



organisations have contracts with equipment providers that binds them to keep environment risk free and even make them liable for penalties for delays and failures

Source: KPMG in India's operational technology survey 2017-2018

Establishing the security of software or devices is easier and more effective prior to deployment, at the time of procurement itself.

Role of sectoral CERT

The government of India established computer emergency response team (CERT) as a centralised body designated under Section 70B of Information Technology (Amendment) Act 2008 to serve as the national agency to perform several functions in terms of assistance and advisory on emergency measures on handling cybersecurity Incidents.

CERT provides regular updates and feedbacks to organisations in various sectors and comes out with specific notifications targeting strategic and critical infrastructure periodically. Organisations should have security procedures tuned-in to these notifications in order to ensure that they are aware of the latest notifications / developments. Sectoral CERT is a working group which consolidate the incident knowledge across various organisations and sectors and then disseminates this information with actionable recommendations to avoid recurrence of such incidents else-where.

When it comes to security event responses, it is imperative for all organisation working in the strategically important ENR sector to be associated with CERT and ensure compliance to notifications issued from time to time. The survey showed:

organisations are neither associated nor aware of sectoral CERT

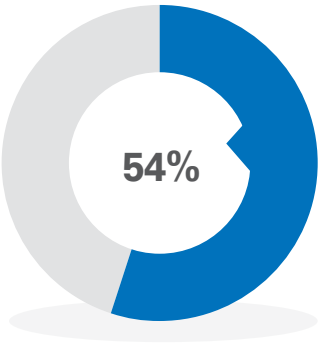
organisations receive security advisory on critical infrastructure from industry specific sectoral CERT and take action / implement advisory as per recommendation

organisations share security information back with the sectoral CERT's information sharing and analysis centre.

Source: KPMG in India's operational technology survey 2017-2018

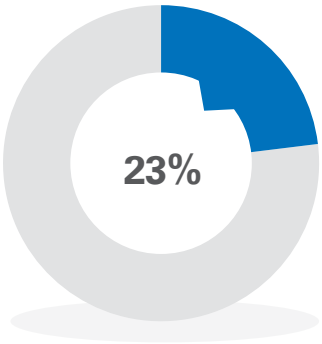
Support required from the government

Having a stable cybersecurity posture in the OT environment is the key for the organisations in the ENR sector. However, most organisations indicated that they require support in various forms to ensure that their systems are secure and cybersecurity incidents are handled effectively. Out of the respondent organisations,

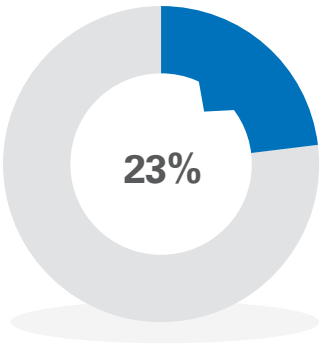


cent agreed that a robust policy should be formulated covering CIS (Critical Infrastructure Sector).

However,

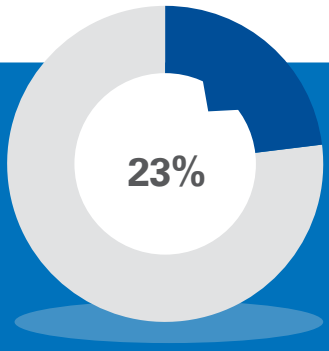


are of the opinion that baseline controls in the policy should be prescribed by government nodal agency such as sectoral CERT. Further, another

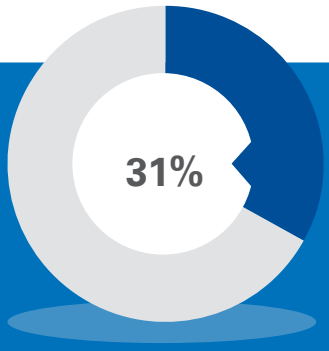


want the increased governance of a regulator, particularly in terms of conducting awareness sessions for the industry.

Under the National Technical Research Organisation (NTRO), NCIIPC has been identified as the nodal agency for the protection of critical information infrastructure. The formal roles and responsibilities of NCIIPC include cooperation strategies, issuing guidelines, advisories and coordination with CERT-IN. Only few (23 per cent) of the organisations have initiatives to reduce risks within their critical infrastructure by partnering with agencies such as NCIIPC, the intelligence community, law enforcement agencies as well as control system owners, operators and vendors.



want an Industry Certification that is focused on cybersecurity in the critical infrastructure sector and believe it can drive the change



expect better collaboration and knowledge sharing on cyber incidents between critical infrastructure industries.

Source: KPMG in India's operational technology survey 2017-2018

Conclusion

Energy and natural resources (ENR) is key sector for country and any disruption not only impacts the economy may also may impact safety and security of the people working in the sector and citizens in the vicinity of the facility. Globally the sector has witnessed major attacks on ICS systems which have impacted services and human lives, while in India we have not seen major attacks which is not by design but by chance as the sector is not prepared for targetted attacks.

The positive aspect which is also evident from survey is that organisations have taken notice of the risks and have embarked on the jounney, which is at various levels of maturity across industy verticals in the sector. The issue is complex and no single stakeholder has capability to fix all issues may it technology and service providers, industry, government and regulators as large number of equipment exists which were not designed and deployed with connected world and cyberattacks at design stage.

Organisations have started to deploy policies and process to address cybersecurity through the lifecyle of usage from design, procurement, deployment and operationalisation of the ICS systems. Government and regulators have also identified the need for security of the sector and NCIIPC is setup. This operates in advisory capacity by rolling out advisories and information based alerts recived from various government agencies. The governing body is yet to travel distance to make it monitoring and governing body which it is mandated for and provide guidelines for each industry vertical as what is setup by TRAI or IRDA or RBI. Industry feels need of support related to awareness and trainings of professional, and guidelines for training and service providers.

Key recommendations based on survey findings are as follows:

- Establish comprehensive cybersecurity framework with clearly defined responsibilities
- Customised trainings for professionals who have been traditionally working in the sector to detect and avert targetted attacks using various social engineering methods deployed by individual with malafide intents and various state and non-state actors.
- Establish connect and regular inter-lock with sectoral and national CERT to take preventive actions and also report the attacks experienced.
- Technology and service provided should be integrated in addressing the risk holistically
- Periodic assessment of readiness from internal and external auditors to test cybersecurity readiness.
- Formal reporting of risks and incidents along with active sharing of information.

CERT-In and NCIIPC publishes alerts and special reports related to critical infrastructure security and provides platform for different organizations to share knowledge and experiences in case cyber security breaches. This immensely helps in providing valuable and timely inputs and enables them to proactively prepare to mitigate the risk.

Acknowledgments

We would also like to acknowledge the core team from KPMG in India who worked extensively in preparation of this compendium:

- Amrit Sethi
- Manish Tembhurkar
- Nikhil Moghe
- Tarun Kapoor
- Monika Jain
- Darshini Shah
- Nisha Fernandes

KPMG in India contacts:

Mritunjay Kapur
National Head
Markets and Strategy
Head
Technology, Media and Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader
Global Cyber Security
T: +91 124 307 4800
E: atuteja@kpmg.com

Anish De
Partner and Head
Oil and Gas
T: +91 124 669 1000
E: anishde@kpmg.com

Atul Gupta
Partner and Head
IT Advisory
Risk Consulting
Cyber Security Leader
T: +91 124 307 4134
E: atulgupta@kpmg.com

KPMG.com/in

KPMG in India 25 YEARS of making a difference

Follow us on:
kpmg.com/in/socialmedia