KPMG

Operational Technology Risk: A View from Internal Auditors

July 2019

kpmg.com/uk

Seven issues for Internal Audit to consider when evaluating operational technology risks

OT comprises industrial control equipment and systems used by organisations automating their manufacturing, processing, logistics, warehousing and R&D. Historically, OT systems were standalone and isolated from corporate networks but this is no longer the case; the prevalence of malware in the second half of this decade has brought to the fore the additional – and very significant – risks concerning OT that organisations are now exposed to.

KPMG recently hosted a debate with Internal Audit leaders from a group of energy, life sciences, transport and manufacturing organisations discussing how they are approaching the risks presented by Operational Technologies (OT). Here are the seven key OT issues we identified.

1. Building a common understanding of OT risks and associated controls across the business

There is a lack of common understanding between assurance and management teams of the differences between OT and IT security risks. Cyber risk and control processes in OT may appear similar to enterprise IT but typically OT controls do not have the same level of maturity. Root causes include:

- The mix of legacy and new technology.
- OT managed within facilities by operational rather than IT staff.
- Networks not up to modern day patching and vulnerability management expectations.
- Unless regulated, not uniformly on the risk radar of Internal Audit.

2. Human behaviours impacting OT controls

Whilst our clients expected OT risks to be largely contained and controlled within the manufacturing/processing facility, they highlighted a risk that inadvertent or malicious human actions could bypass such controls and put the enterprise at risk.

One organisation told us that OT vendors have been seen running patches from USBs, even after multiple USB-related malware incidents had been reported across the sector. Another client explained how complacency can set in, leading organisations to think that OT controls are adequate and operating; somewhat like a driver who 'switches off' and relies for their protection on motorway variable message signs that may not actually be working.

Companies from the power and mass transit sectors described how social engineering can still be used to get round barrier controls simply by appealing to staff's sense of 'being helpful'. With such uncertainties over the strength of physical and OT controls, OT risks could have just as much, if not more, impact than IT risks.

3. Impact of new technology on OT risks

New operational technology, such as Industrial Internet of Things (IoT), is commonly layered on top of legacy systems that are several years or even decades old, often presenting prohibitive cost and disruption to the business to upgrade. Legacy operating systems can present a major OT risk.

A stark example was given of OT on Windows operating systems that were two generations out of support. One client emphasised that whilst major incidents like Wannacry and NotPetya force the business into immediate action, momentum can quickly subside and there is an imperative to get the business to take sustained action.

Yet some cost and disruption seemed inevitable for the options to reduce OT risks. Options ranged from wholesale OT equipment upgrades, to a combination of phased OT upgrades with strengthening of existing controls. Strengthening existing controls might mean enhancing the monitoring and security operations, as well as redesigning and regularly testing recovery plans. Internal Audit is ideally placed to help identify options that minimise cost and disruption whilst protecting the business from lost revenue, loss of customers, and even fines from unplanned events.

4. Impact of evolving regulation in OT

Some of our clients' businesses operate under tight regulations designed to safeguard the quality and availability of their products. Clients from pharmaceuticals and energy sectors don't rely on just regulation to set their risk tolerance. For those clients the OT risks could have real impacts to life and health, requiring sophisticated controls. Our clients working under the recently implemented Network and Information Systems (NIS) regulations told us of their uncertainties in how regulators will act on the mandated gap assessments required of their organisations.

Internal Audit can play a key role in helping identify where regulations apply to OT in their businesses, checking management's compliance with such regulations and engaging in the debates where regulation affecting OT is evolving.

5. Impact of vendors in OT risks

It is imperative that management start to challenge OT vendors to bring OT security risks into tolerance, for example through agreeing roadmaps for remediation. There is a relatively small set of big OT vendors, which means it might be more efficient and more effective for organisations to think about coordinating their approach to tackling individual vendors rather than leaving it to each of their respective business units. Internal Audit can play a key role in assessing the vendor-managed side of OT risk.

6. Gaining assurance over OT risks

Some Internal Audit teams run regular site-based audits of OT controls and include physical controls. When operating critical infrastructure, power companies face multiple security audits by third parties. In addition many organisations face the complications of gaining assurance over joint ventures, particularly where they're not the operator and are therefore less able to direct the agenda. However, there are examples of joint venture audits with a focus on financials that are now also addressing some OT risk.

When resources are in tight supply and audit committees have not previously considered OT risks, some client Internal Audit functions face significant challenges in getting support to resource OT audit work in their annual plans. Such challenges may, in part, arise from Internal Audit having too little data on the scale of the OT risk to highlight a need for an independent audit check on the OT risk management.

7. Sourcing OT skills for audits

Accessing the specialist OT skills for OT internal audits is tough with few options. OT audit skills can be built by training, or SMEs can be sought (e.g. from management's OT teams if conflicts of interest can be resolved). Organisations who do internal audits on OT may have to rely on SMEs from the business or consultancies. Without the flexibility to offer attractive career paths, or budgets that allow competitive salaries, most Internal Audit functions can't maintain or grow OT expertise efficiently.

The EU launched the network and information systems directive in 2016, requiring all EU Member States to introduce cyber security legislation for the protection of critical national infrastructure. The UK government therefore launched the Network and information systems regulations 2018 which came into force on 10 May 2018. This was the first time many UK industry sectors were formally subject to cyber security regulation. Completion of the government's Cyber Assessment Framework (CAF) by each affected organisation is designed to demonstrate compliance, which can then be validated by the 'Competent Authority'. Maximum penalties for non-compliance are currently set at £17 million.

The key OT concerns we developed with this group demonstrate how Internal Audit can help management address this critically important risk area. Internal Audit is uniquely placed to identify gaps in OT controls, along with remedial actions that protect the business from lost revenue, loss of customers, and even fines from unplanned events. The aim is two-fold: getting the right, systematic action by management, and getting the right, focussed assurance to the Board.

How can KPMG help?

Understanding the risks you're currently running, including those driven by emerging technologies, and what you could do to help control those risks, is critical to managing a business dependent on OT. Whether that's people risk, compliance with legislation or understanding how vendors impact your risk profile, organisations must manage the risk. Talk to your regular KPMG contact or get in touch with Andrew, Paul or Jaco to discuss this topic in more detail and see how KPMG can help you gain control over this critical area.

Contact us

Andrew Shefford
Managing Director
M: + 44 (0)77 7570 4613
E: andrew.shefford@KPMG.co.uk

Paul O'Sullivan
Senior Manager
M: + 44 (0)77 7500 7254
E: paul.osullivan@KPMG.co.uk

Jaco Benadie
Senior Manager
M: + 44 (0)79 2036 1766
E: jaco.benadie@kpmg.co.uk

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by CREATE | June 2019 | CRT115891A