www.pwc.com.au

Internal auditors can help protect against the growing wave of ransomware attacks

August 2021

Internal auditors can help protect against the growing wave of ransomware attacks

Australia's internal auditors have been rightly lauded for anticipating, identifying and responding to business risks. In recent years, the profession has been instrumental in transforming financial, non-financial and governance processes in organisations of all shapes and sizes. Now, in 2021, it's vital that internal audit teams step up once more. They must apply their skills and frameworks to a risk that can bring any organisation to its knees.

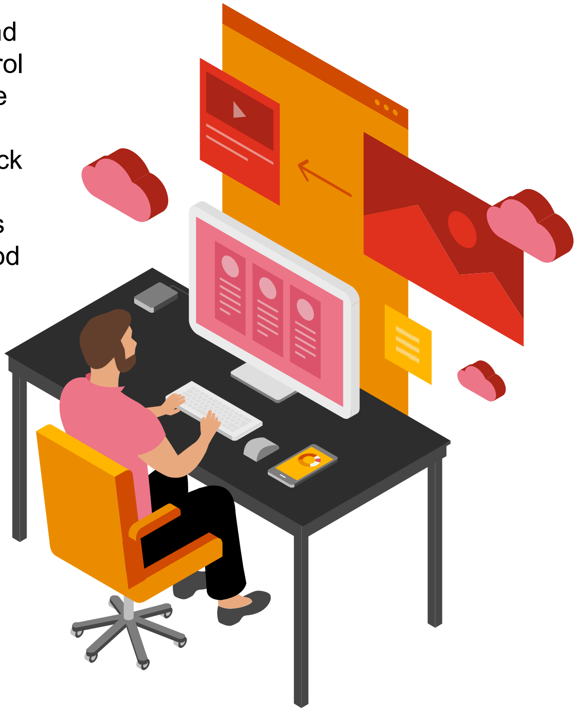
The cyber threat landscape (and associated regulation) is growing fast. Organisations should ensure ICT systems are robust with the right governance, policies and controls in place. In doing so, they must focus not only on processes but also on technology and the people who use it.

As we explored in a recent PwC internal audit webcast, cyber threats come in many forms and one of the clearest and most present dangers is ransomware. It's imperative that internal auditors stay updated on how ransomware attacks are evolving and how these could impact their organisations.

Alarming increase of ransomware attacks in Australia

Ransomware attacks are increasingly sophisticated, and no industry or organisation is completely immune. It has become a weekly, sometimes daily occurrence, to learn about leading organisations across Australia that have been significantly impacted by a cyber breach that's halted their ability to conduct business.

When a ransomware attack pierces an organisation's defences, there are one of two outcomes: Either the organisation takes the contentious decision to keep quiet and pay criminals an eye-watering sum of money to regain control and security – or the organisation refuses to pay, reports the crime to the authorities, and suffers the damaging consequences of the attack. Either way, a ransomware attack could cost your organisation dearly. And the bad news? These incidents are on the rise and Australian organisations can be a soft and lucrative target. (But we'll come to the good news shortly).



For internal auditors, this means that your organisation may already be subject to cyber compliance and reporting obligations or – if it isn't – it soon could be. So now is the time to demonstrate that you're ready and able to comply.

Understandably, governments are giving more and more attention to ransomware attacks. In Australia, pressure is mounting for a mandatory reporting scheme. The current legislative regime is complex, encompassing state and federal rules as well as industry-specific requirements from the likes of ASIC and the ACNC. Meanwhile, US President Joe Biden is stepping up his nation's cybersecurity and calling for international cooperation from allies.

Showing that your organisation has its guard up is not only good from a regulatory perspective. It can be a powerful deterrent for malicious actors, who prefer easy targets. And it sends a strong message to your customers and supply chain: that you're less likely to expose them to cyber risks.

Questions board directors should be asking

Cyber risk is shooting up the agenda for boards and executive teams, and their conversations with internal audit leaders typically raise a variety of pertinent (and often challenging) questions:

Strategy

What are our organisation's top three cyber risks? Did we consider cyber risk last time we discussed our digital strategy? How confident are we that we understand all the ways we are exposed to cyber risk?

Board ownership

What is our largest cyber security gap? Which of our third parties have best practice controls in place? Do we know who our most risky third parties are and why? Have we sufficiently considered the impact of our cyber risk profile in board discussions and decisions? Are we simplifying our operational complexity enough to make our organisation more secure? Do we have the necessary capabilities to discharge our technology and cyber duties?

Executive accountability

What are our cyber risk responsibilities? During a cyber incident, what would our personal roles be? What legislative requirements are our organisation subject to and what are the obligations for our executive team?

Financial resilience

How would a multi- million cyber event affect our organisation? How much capital do we have in reserve for cyber events? Would we pay a ransom?

Reporting

How do we report our cyber risk position to the board? As a result of that position, what actions have we taken? Are we aware of the actors currently attacking our organisation, what their interests are, and how successful they've been?

Assurance

When was our last independent report for cyber? What was the outcome? What compliance framework do we use for cyber? How does cyber fit within our enterprise assurance/risk framework?

Questions board directors should be asking (cont'd)

To form robust answers to these questions, internal audit teams should look at cyber holistically across their organisation's processes, technology, and people.

ICT systems and processes need to be sufficiently secured to ensure that the information within them is safe. For internal audit, this doesn't require a deep technical understanding of the underlying code behind technology; but it does mean seeking evidence that the right governance and controls are in place.

And the focus on people is absolutely critical too. When we polled internal audit leaders and managers at our recent webinar, approximately half pointed to 'the human factor' being the single biggest cyber risk for their organisation. Recent analysis found 85% of data breaches involved human interaction.

Often human interactions aren't deliberate acts of sabotage or malfeasance, but accidental errors. So, it's vital that people are trained and understand the rules and controls that are in place.

Common and recurring gaps

It’s hard to conduct an internal audit without a clear map of what to review against. Fortunately, Australian best practice is widely available from the Australian Cyber Security Centre (ACSC), which sets the gold standard for public and private sector organisations alike.

When reviewing governance and controls, internal audit teams will invariably identify areas for development or remediation. Common and recurring gaps often include failure to:

1. Develop appropriate risk management
2. Develop a strategic plan for ICT
3. Plan for a cyber event
4. Convey important and urgent gaps to the executive

Common and recurring gaps (cont'd)

By openly and transparently assessing ICT risks, it's possible to defend against them. To inform their risk assessments, internal audit teams need to understand who likely cyber adversaries may be. This helps tailor the assessment for the organisation and avoid a generic 'box ticking' exercise. Depending on your organisation, perpetrators could be an organised crime group, a nation-state, social/political activists, or internal staff. Each of these actors have different motivations and techniques, and the controls that organisations need to implement may differ for each actor.

With almost all enterprises relying on technology for day to day business, development of an ICT Risk Assessment enables the careful consideration of the adequacy and criticality of key controls within these systems. Consideration needs to include open and transparent consideration of system weaknesses, possibility of manual circumvention of controls and how the actions or inactions of both internal and external actors may impact on outcomes. Critically an ICT risk assessment should enable the prioritisation of ICT projects and mitigation strategies based on the assessed level of risks to information or key systems. Feeding into the ICT strategic plan.

A strategic plan for ICT is essential too. Not only for hygiene and safety reasons but also because it may be mandated by authorities (e.g. the ACSC requires this for many government agencies). The ACSC has published eight baseline mitigation strategies applicable for most organisations, be they public or private. This includes suggested tactics to make it harder for adversaries to compromise systems.

As organisations continually upgrade and refine their cybersecurity defences, hostile actors will continue to seek new ways to infiltrate these. So, it's prudent to prepare for the worst-case scenario – just in case. Comprehensive responses to a cyber event include activating business continuity plans, rapidly closing attack vectors, issuing communications with stakeholders, meeting reporting requirements (e.g. OAIC for information breaches), and retaining evidence for investigations.

As and when major gaps are identified, these need to be shared with the executive team in a timely and succinct manner. ('Techno babble' is more likely to confuse senior leaders, rather than inform them). Risks should be linked back to organisational objectives, and executives should be informed of relevant legislative obligations and personal liabilities.

And finally, the good news. As we've outlined, there's no shortage of cautionary tales in the media about ransomware attacks and their crippling impacts. (Doubtless, there are many more incidents that go unreported). But the good news is that internal audit teams have access to the skills, expertise and frameworks to help their organisations prepare and respond to these threats, and reduce the chances of their organisations hitting the headlines for all the wrong reasons.

For more information, feel free to reach out to a contact below or learn more via one of the links below.

Contacts

Sophie Langshaw

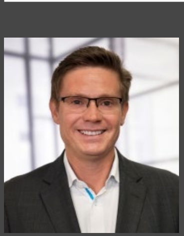
National Internal Audit Leader

+61 410 520 548
sophie.langshaw@pwc.com

Robert Di Pietro

National Lead for Critical Infrastructure Security

+61 418 533 346
robert.di.pietro@pwc.com



Craig Sydney

Partner, Sydney, PwC Australia

+61 400 215 757
craig.sydney@pwc.com

Register for future IA Information Series sessions

Read findings of PwC Australia's Digital Trust Insights 2021 survey