Queensland Audit Office
Better public services

Cyber risk: what do we do now?

QAO podcast transcript

Joel Godwin:

Welcome listeners to the Queensland Audit Office's inaugural podcast titled *Cyber risk – what do we do now?* I'm Joel Godwin, Senior Director responsible for our performance audit reports to parliament and I'll be one of your presenters today. So QAO, we're in a really unique and privileged position where we actually have touch points annually with all public sector entities across Queensland.

And today we're going to look to draw on many years of work in both cyber and IT space, together with our most recently tabled audit report titled *Responding to and recovering from cyber attacks*. We've got some really interesting advice and lessons to share today. We actually ran some cyber attack simulations with audited entities, which was a great exercise.

And overall, just really what a topical area to start with in cyber. But before we jump in on that, I'm delighted to welcome QAO's Senior Director for Information Systems, Sumi Kusumo, and our guest presenter, Robert Champion, Chief Information Security Officer from the Queensland Government's Cyber Security Unit.

Welcome Sumi and Rob.

Sumi Kusumo:

Thank you, Joel. Nice to be here.

Robert Champion:

Yeah, great to be here. Thanks, Joel.

Joel Godwin:

So to kick off today's conversation, I thought it'd be great to hear from you, Rob. So, as I mentioned, cyber, it's such a topical area. It's a high priority for all organisations, both public and private sector, whether you're big, whether you're small. And I feel like every week there's a new cyber attack coming out somewhere and those are only the ones we hear about.

So we always say around the office, it's not a matter of if, but when.

Robert Champion:

Yeah, Joel, definitely a deteriorating threat environment that we find ourselves in. You'll read in the news most weeks, major cyber security attacks happening against big organisations and government and a whole range of small organisations being hit as well.

Every 6 minutes somebody's reporting a cyber attack to the report cyber line. That's up from one every 7 minutes last year. Cyber criminals, foreign governments, internal actors – all have intended and unintended consequences across our organisations and we need to protect ourselves from these.

It's really a matter of time before each organisation is attacked, and the question really is how do we protect, prevent, and respond against these attacks?

Joel Godwin:

Yeah, great. A really fast-moving environment here in the cyber space. So a key message for me that we're going to touch on a number of times throughout today is that each entity really has to take responsibility for the management of their own risks in cyber.

There's some really great support and resources around which can help entities, such as the great work that Rob and his team at CSU do. The buck really does stop with the chief executive officer and those charged with governance. So I might start by throwing over to you, Sumi. What do you think entity leaders should be doing now to prepare themselves?

Sumi Kusumo:

Well, organisations now need to be cyber resilient. Meaning that they need to have not only controls to prevent a cyber attack from happening, but also they need to have the ability to detect an attack is happening and then respond and recover from the attack. Previously, many organisations focused on preventative controls.

But as you know, 100 per cent protection is not possible. Hackers only need to get it right once to breach your system, while IT security or your organisation actually need to get it right all the time. Now some of these preventative controls are basic security hygiene that is still relevant in managing cyber security risks.

We are continually identifying weaknesses in entities' information systems, such as not restricting privilege or full system access. Only give this this level of access when absolutely necessary and disable access when account has not been used for an extended period of time. And also, some insufficient cyber security training for staff. Methods that actually we should all be on top of it by now.

Joel Godwin:

Absolutely Sumi, and what would you say is the essential starting point for an organisation to do this?

Sumi Kusumo:

An essential starting point for an organisation is to have a complete understanding of their critical systems and information assets. Assets are known as your crown jewel. So know the value of your systems or your data to your entity, to your stakeholders, and to the adversaries who are interested in your data, and then have a risk management strategy for your crown jewel to make them more cyber resilient.

Robert Champion:

Yeah, definitely. Sumi. It's knowing the value of your system and data is really important, as you said, to the stakeholders and to the adversary. Knowing how the adversary can use that information downstream. One breach in an organisation can lead to tens of thousands of downstream incidents. And it's that visible impact security and organisations and police are aware of.

It enables other crimes, not just that original crime through identity theft and other attacks.

Joel Godwin:

And so to me that probably touches on our first theme of the day which really comes back to the basic principles of risk management. A really key starting point here is understanding those critical systems and information assets which are valuable not just to you but to external parties as well, which Sumi sort of touched on before.

Yeah and once you know that you can really then assess how well the risks to those systems are being managed. So in our recent work on responding to and recovering from cyber attacks, this was an area where we found that some entities were not doing this often enough and perhaps their understanding was a bit outdated.

And really if you, if you don't understand your risks and don't understand your vulnerabilities then how can you be expected to plan to protect those properly? Once you do know your risks though, it becomes a matter of how do you plan effectively and respond to those. And there's a few different layers to that which we'll talk through. And Sumi probably touched on them earlier, but really the first layer of having those appropriate system and preventative controls in place to ensure you're preventing an attack – so you need to lock the house up so no one can get in. But in the case that someone does, that's where it's really important to have key plans in place such as incident response plans, which are there in the event of an attack. And this isn't just about technical areas like disaster recovery.

It's about how the whole organisation comes together to respond. Which again is another theme we'll talk through today – cyber attack needs to be treated as a business first problem, not a technical problem. These plans are there to help bring the organisation together and how you respond to an attack and really they have to integrate with some of your other key risk documents such as your business continuity plans and your disaster recovery plans.

Robert Champion:

Cyber attacks are foreseeable events, we can see them happening in other organisations, you can read about them in the news. Opportunity to learn from each of those, take what we hear in those situations and test our assumptions in the organisation at an audit and risk committee level. We should be able to understand our exposure, our posture, and the threat and risk environment that we're in. And is it changing?

Joel Godwin:

And staying on risk, one of the other key areas our report did highlight was actually the management of third-party risks. So, for example, those systems which are managed externally to your organisation but still hold critical information for you. None of the entities we audited actually had strong arrangements in place to understand and manage these risks.

But these are really the common areas where threat actors find their way in in a cyber attack. Sumi, you'd see this pretty regularly in your work, wouldn't you?

Sumi Kusumo:

Yes, I see this often. When third party vendors provide hardware and software or IT services, they need to become part of your risk management framework.

So you need to know how to use these vendors, you need to define the appropriate contracts, and then continually assess how well each of these vendors actually managing their securities and responding to those attacks as well.

Joel Godwin:

Yep. And we touched on it earlier, but executive management really does have to have responsibility for those risks and all those external suppliers.

So each entity has got to be satisfied that those third-party arrangements are adequately reducing the risk to an acceptable level. Quickly, before we move on, one last interesting area which sort of came out of the audit was around cyber insurance arrangements. So these are essentially a risk mitigation strategy put in place by entities.

Just to be clear, they don't mitigate the risk of an attack, they aren't there to manage brand damage or reputational damage or legal damage, they're purely there as a control to manage financial risk. So, they are quite commonly used, both within public and private sector, however it's really important that if you have these arrangements, you understand those specific clauses and escalation points within those contracts.

What does it cover? What does it exclude? And one thing we saw in our audit is that these were not always well understood by entities. So, like all insurance arrangements, there are complexities to it and you need to understand particular clauses. Otherwise, you risk having your financial controls voided.

Sumi Kusumo:

So Joel, an attack occurs. What will be your recommendations for organisations to respond and recover from this attack?

Joel Godwin:

Great question. I think that was one of the really key recommendations which came out of our report was around entities needing to test their preparedness more regularly. So I think of all the entities in our audit, only one had actually run simulations before and tested their plans.

So, in the event of an actual attack, things will move really quickly. So, decisions are going to need to be made, you're going to be under pressure, it's going to be a stressful environment, – a lot of time pressure on individuals and the overall organisation. So, it's one thing to have a plan in place, but these need to be pressure tested through activities such as cyber incident response simulations.

And to touch on a sports analogy, it's like having a footy team. You can talk, you can plan, you can get out the whiteboard all you want, but you need to test how these are going to work in a game day simulation under pressure if they're going to actually be effective.

So, in our audit, we held these exercises with all 3 entities to test how their key personnel, both technical and non technical, responded. Look, and these were really great exercises. They put key management and key personnel really under the pump to test their readiness. And I know personally, I was very glad to be on the other side of the table to watch them, because even though they're only a simulation, they were still quite stressful.

But I know we got a lot out of those exercises, and speaking to the entities after, they also got a lot out of them. So, really great process to run as well. Rob, I'd love to get your views on how valuable these exercises are.

Robert Champion:

Yeah, we see these as being really key ways of bringing the team together around the incident response. Helping the organisation understand not just technically what would occur during an incident, but also how decision making will be made, how risk assessment will be done at that time, how we improve our security measures, and how do we learn lessons through that exercising.

As you said, it is simulations – an opportunity to do that in a safe way. We've run whole-of-government exercises for the past few years. Really what that tells us is that there are more to it than just the technical response. How we communicate with our customers, how we communicate with stakeholders, legal implications, also, our service delivery obligations to our customers, really important. It's an opportunity to educate, not just to validate the plan.

Joel Godwin:

And obviously these simulations, they test a specific scenario and we know that all, obviously not all cyber attacks are the same. So what scenarios should entities be planning and testing for?

Robert Champion:

So definitely there's a range of scenarios. They include email compromise, ransomware, data breaches, supply chain incidents. But there's a lot of variability to what's going on. We can look at what's happening in the media and come up with additional scenarios on a day-to-day basis.

Joel Godwin:

And so to move on to some of the lessons we got out of those. So we found that those entities who took a business-led approach were better at coordinating their response. So they looked at the broader organisational impacts rather than just the technical systems and technical rebuild. So to respond, you're going to have to bring in key stakeholders from parts of the organisation like legal, communications, operational areas, and they need to work hand in hand with the technical teams in the event of an attack.

So to step it back, your plans obviously need to incorporate all these areas, and then you'll need to come together to test how they work in a real life situation. Some of the other probably basic learnings which came out of it were even having hard copies available of your plans. So obviously we all live in an electronic world these days, but in the event of an attack there's a good chance that your laptops may be out of action, so you need to think about how am I going to access these plans if I can't access my computer.

Sumi Kusumo:

So we learned from the simulation exercise that to move effectively and quickly during an incident, you must be clear on who are your stakeholders, who is responsible for what, who need to do what, and articulate this in your incidence response plan.

Robert Champion:

These simulations are a great way to get intelligence and share risks, and test those assumptions that we have across our systems and our organisations. But also to share them more centrally across the sector.

What happens in one organisation may be a theme that others can learn on as well. Taking back to your team sport conversation before, Joel, really it is – cyber security is a team sport. We are all playing on the defense. We need to share lessons learned amongst ourselves on how we do that.

We also need to move as the threat environment changes. So the goalposts move. For example, backups and the controls we had in the past – backups were really around the loss of hardware or software, now we have motivated attackers that come in and will delete backups out of your organisation. So the control that we had in the past is no longer effective against the systems threats that we have today.

So it's no good just to have a backup. You need to be able to recover from that and you need to have tested the ability to recover from that. Not every incident is going to be in the control of your technical experts. Some of those controls will be elsewhere, either in partners, other parts of government, in your supply chain.

Joel Godwin:

Probably one last lesson which I'd like to highlight from our simulations, which we commented on in our report, was around having effective crisis communication plans in place. These are really helpful and they detail how you'll engage stakeholders, not just internally, such as your employees and management, but externally with customers, suppliers, regulators, oversight bodies.

As we've sort of touched on, you don't want to be deciding what to say under pressure, so these are really critical in managing the right messages to the right people at the right time. These plans really do help clearly document thresholds for decision making as well and the communication protocols you'll need to ensure escalation of an incident at the appropriate levels.

Robert Champion:

So definitely knowing who to reach out to in an incident is really important.

Cyber security unit, response capability, can assist centrally for agencies. So we have a range of technical and advisory services that we can provide to agencies experiencing an incident. So we can help you know who to engage for help in regards to both legal comms, technical, but it also gives us that opportunity to give you boots on the ground, or advice at really short notice to be able to deal with that incident.

It's not necessarily something that the day-to-day team will have a lot of experience with, hopefully.

Sumi Kusumo:

So, we have talked quite a fair bit about managing cyber security risk so far. Joel, at the end of the day, who is accountable for managing cyber security risk?

Joel Godwin:

Thanks, Sumi. So as we touched on earlier, responsibility to me really lies with the chief executive or equivalent.

It's not something you can assign externally. And, as you know, as we touched on at the start, entities need to own their risk and be accountable. But to be honest, it's not quite as simple as just that. So, good executives are going to own their risk, but also know who to get advice from during an attack.

Who are the experts? Who can I bring in to help me? They should have the right structures in place and the right people around them to get the assurances they need that things are being managed.

Sumi Kusumo:

So everything we've covered today is fundamental to good governance. And managing cyber security risks need to be part of the behavior and culture of an organisation.

It's not something that we've got in a document or in a plan and so on, but something that we need to be actively managing the risks.

Joel Godwin:

Yeah, that's a great, that's a great call out. So governance committees are really critical in the management of cyber risk and, and to be honest, they need to be treating cyber risk just like any other risk.

It just happens to be a really fast moving one and one that can have a huge impact on your organisation if not managed. So boards and governance committees have a really important role in ensuring that their entities have the right defences in place and the right culture and resilience across the organisation.

These days, cyber should really be an agenda item for all committees. It's not just about the chief information officer managing this risk. They need to be across the detail. They need to understand what's being done in that space. And ultimately it should be treated, as I said, like any other operational risk and be regularly discussed.

Even these days, most committees, if not all committees should really have cyber expertise embedded on them. So you need to have the right people there to ask the right questions of management to know that the things are being managed appropriately.

Sumi Kusumo:

What resources can we offer our listeners today, Joel and Rob?

Joel Godwin:

I'll probably start first if that's alright, Rob. So alongside our report on responding to and recovering from cyber attacks, we actually provide guidance for those charged with governance. That's really executive leadership and governance committees and boards. So what we've included is a 2-page resource with some key questions leaders should be considering with respect to their cyber security, incident response, and recovery.

We also provided within the report a role capability guide. Really that's there to help you prompt about what you need to think about from a skills and capability perspective. So where do you hold those skills and capabilities within or external to the organisation across both people, processes, and technologies.

So entities can discover and note when they were last tested and address any gaps through this guide we've included. Outside of these though, Rob, did you want to talk about what you've got in place at CSU?

Robert Champion:

So definitely. CSU has a range of services and assistance we can provide to organisations before, during, and after cyber incident.

We provide a range of technical services that agencies can take advantage of – vulnerability scanning, some email hygiene services, phishing and user awareness services. That helps an organisation understand where they're sitting at. We also are pulling together more of that information to be able to take up to a governance level so that the non-technical audience can start to understand the posture of the organisation.

There's a fair bit of guidance under the IS18 policy framework. All of this can be found on the Forgov website if you search for the word cyber.

Sumi Kusumo:

In our new forward work plan, we have some future audit topics and reports on managing third party cyber security risks and protecting information held by government.

Keep an eye out and check out QAO's blogs on topics such as cyber security and also risk management.

Joel Godwin:

Such a big topic and a lot of learnings, but unfortunately that's all we have time for today. So, a big thank you both to Sumi and Rob for joining me. Big thank you to our listeners. Please do send us your feedback on our chat on our website.

But overall, this is the Queensland Audit Office sharing insights for better public services.

Bye for now.