How the **City of Onkaparinga** survived a shocking ransomware attack

The City of Onkaparinga is the Australian state of South Australia's largest metropolitan council. It is one of the state's fastest growing areas and the Council's staff support 170,000 residents as well as a diverse range of commercial and agricultural sector ratepayers

CUSTOMER-AT-A-GLANCE

CITY OF ONKAPARINGA

Company Name
City of Onkaparinga

Industry
Local government

Number of Users
700+

Sophos Customer
Since December 2019

Sophos Solutions
Sophos Intercept X Advanced
Managed Threat Response

'Sophos and its partner had the best people from Australia and around the world working all hours to help bring us safely back online. They were fully prepared and across all the issues. With their combined expertise, they've also been absolutely essential to the preparation of the incident's forensic analysis and our insurance claim.'

Desma Morris, Manager ICT, City of Onkaparinga

How do you combat a ransomware attack just before Christmas?

Australia's City of Onkaparinga Council was paralysed in a targeted, high impact ransomware attack that resulted in lost productivity, unbudgeted costs, immense stress and a very steep learning curve. The first obvious signs of the cyber-attack appeared on Saturday 14 December 2019 when the Council's email system shut down. The incident rapidly escalated to include a complete server outage, limited end-user computing capacity and no access to VoIP phones. Not only were the Council's central operations hit but all community services such as libraries and support hubs across suburban and rural areas were crippled as well.

Investigations identified the RYUK cryptolocker virus had infiltrated its ICT environment. This particularly vicious strain of cryptolocker, paralyses organisations in multi-stage incidents. RYUK monitors the host, gets into the system and lies dormant before enabling the hackers to take over administration privileges to delete and encrypt critical files.

The targeted sophistication of RYUK's phishing campaigns deceive staff with what look like genuine internal emails. The City of Onkaparinga ICT Team Leaders Kym Groves and Zoran Bancevic explain: "The RYUK emails were addressed directly to our people, covering topics they were working on. When everything looks normal, busy people are going to click on attached documents to be actioned. And when there's no immediate system issue, no danger signals are flagged."

The initial attacks would have been short lived to not arouse suspicion. As the emails were distributed throughout the organisation, contact lists were compromised. But nothing would have registered in the sent or Exchange logs.

Once RYUK activated on 14 December, Onkaparinga's ICT team spent four sleepless days and nights battling the incursion. As backups from the Friday were reinstated, a new attack at 1.30am each night closed everything down again.

"It was insane chaos over the first few days, however because our backup data was not encrypted, we were confident we could get systems back but we badly needed boots on the ground to help. And we didn't contemplate opening any files that may have contained a ransom demand because our backups were protected. We contacted

our original anti-virus vendor and they told us they couldn't help; we were on our own. Their response was terrible," said Desma Morris, Manager Information Communication Technology (ICT).

When is it time to call in the experts?

On the Monday following the system shutdown, the Council's crisis management plan was enacted.

"We had access to nothing and had to act fast. CompNow, our IT service provider, made the case for Sophos Intercept X Advanced Managed Threat Response (MTR). They negotiated a 90-day licence to fix the immediate issue and prove its value to us for an ongoing subscription," Ms Morris says.

Standard managed detection and response (MDR) services stop at notifying customers of potential threats. Sophos MTR offers the additional service of response experts taking targeted actions to neutralise even the most virulent attacks.

From Sophos' global network of security operations centres (SOC) its cloud-based software actions were initiated to remotely disrupt, contain and neutralize Onkaparinga's RYUK incursion. Conference calls between the local teams and Sophos' UK SOC shared vital visibility into the environment and the evolving solution.

The seriousness of this attack cannot be understated: "If they target you, they will get in – unless you have specifically designed, up-to-the-minute, 24/7 protections against these types of complex attacks," Ms Morris says.

While the Sophos MTR team investigated the source and tendrils of the hacking, CompNow was on-site at the Council until late December. With Sophos installed on critical servers, the vital email, finance and property systems were restored on Wednesday 18 December.

"The virus hit just before our pre-Christmas pay run – the largest of the year, with all the leave entitlements. We were determined to get our staff and suppliers paid so getting Payroll and Accounts Payable up was vital," Ms Morris says.

"On the 18th we had our first successful stop of RYUK's daily 1.30am re-encryption. It had been a really tough time but having the extra CompNow and Sophos engineers on board took the load off our really stretched internal team. With our pay runs completed, things started to look a little brighter."

For staff returning to work in early January, on-site kiosks were set up to scan their laptops, external storage devices and cameras. RYUK and bot files were found in 60 devices.

What are the benefits of a managed threat response solution?

"We could have been completely overwhelmed and confused through this stressful time. Everyone had their own urgency – but we didn't have the expertise or the capacity to address all the issues at once, we had to stick to our priorities. CompNow and Sophos supported us, gave us the expert authority to work through what we needed to do. The demonstrations and forensics provided by the Sophos SOC were clear and extremely helpful. The solution worked like a dream, it gave us breathing time so we could be productive," Ms Morris says.

The recovery project had a very important measurement of success. In the continuous monitoring of the Council's environment over the three months following the breach, there was no evidence of any personal data being accessed.

Onkaparinga converted the proven 90-day interim Sophos licence to a three-year contract. Sophos Intercept X is loaded on each of the Council's 131 servers and 1265 devices. It is remotely, automatically updated and managed via the cloud and the IT team monitors activity from a central dashboard.

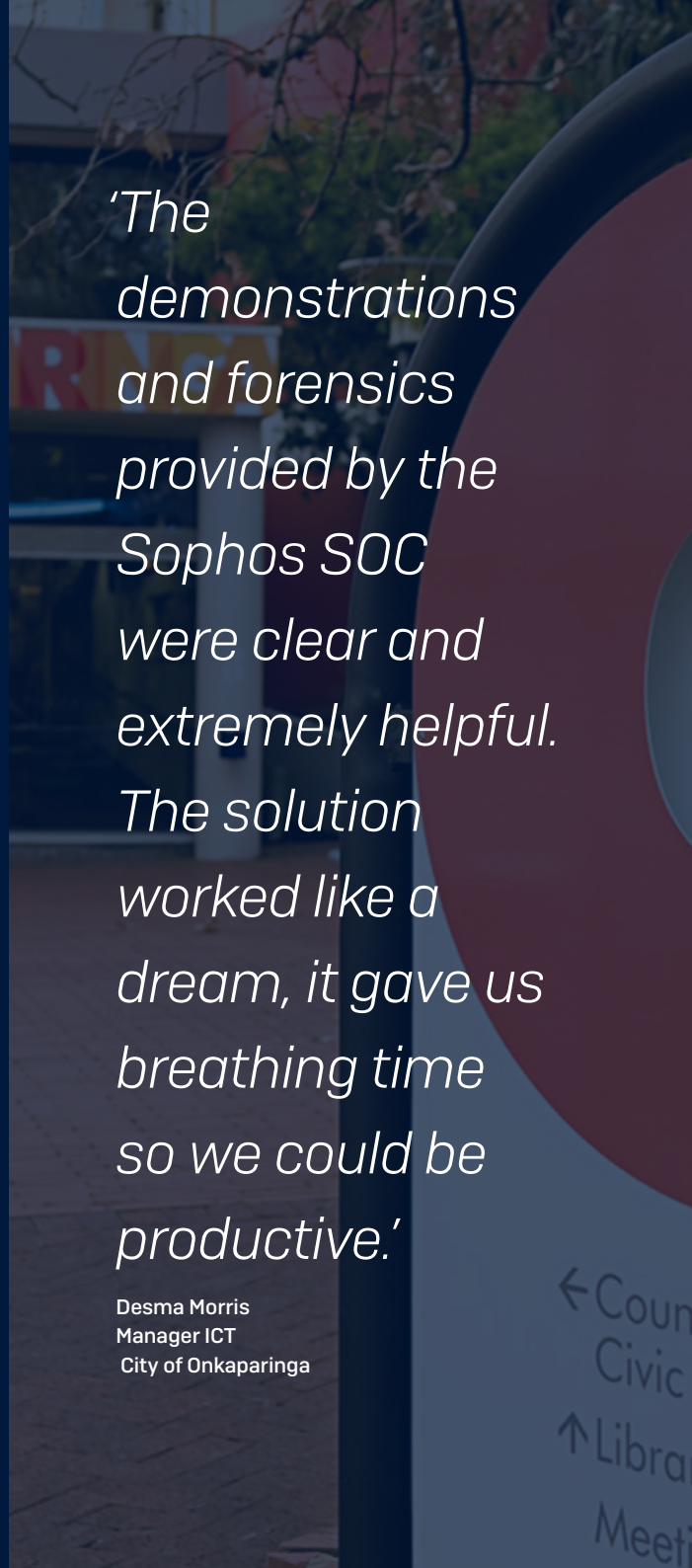
"It's not feasible for someone sitting in a Council IT team in Adelaide to be awake analysing and defusing the 400,000 fresh malware threats that appear every day. Sophos is monitoring the traffic on our network and status of all devices 24/7 and can remotely isolate any infection. We can get on with running the systems for our Council knowing they'll be up and clean when we need them," Ms Morris says.

The City of Onkaparinga undertook a comprehensive review of the three-month incident and recovery process. Its revised ICT disaster recovery plan – with Sophos at its core – ensures it can remediate and protect its business-critical environment into the future.

Sophos MTR Advanced ensures cost predictability for the Council as the managed service is all-inclusive without any per-incident related costs like other managed threat services.

"As a lesson learnt, I can't stress too highly the need to regularly test your crisis management arrangements – with your trusted partners. And you don't survive something like RYUK without the full support of your executive," Ms Morris said.

With the advent COVID-19, Sophos continued providing security peace of mind. Staff working from home, often from personal rather than Council devices, had the same enterprise level protections as working in the office.



'The demonstrations and forensics provided by the Sophos SOC were clear and extremely helpful. The solution worked like a dream, it gave us breathing time so we could be productive.'

Desma Morris
Manager ICT
City of Onkaparinga

SOPHOS