Case Study

Coventry City Council
Local Government
RansomCare

Coventry City Council protects citizens, staff and services with best-in-class ransomware defence from Ricoh

Coventry City Council was increasingly concerned about the growing threat of ransomware attacks. The start of COVID-19 lockdown sharpened focus on the risk since good security practice was difficult to apply on staff working from home. To ensure the best defence, the council decided to deploy Ricoh's RansomCare solution a decision which it described as 'a no brainer'.

Executive summary

Name: Coventry City Council
Location: Coventry, West Midlands
Size: 5,500 staff
Activity: Local Government

Challenges

- Growing threat of ransomware attack
- Risk to service continuity and high cost of recovery
- COVID-19 and homeworking exacerbate the problem

Solution

- Ricoh RansomCare
- Ricoh expert consultancy

Benefits

- Delivers one of the best defences against ransomware
- Protects against extra threat of staff working remotely
- Offers value for money vs. damage and cost of attack
- Fast and simple to install, just half a day
- Has minimal impact or intrusion on IT infrastructure

Challenges

Coventry City Council is a unitary authority responsible for providing local government services to 360,000 people in the city. It is nominated as the UK City of Culture for 2021. The council has implemented a digital transformation programme to improve the operation and delivery of services to the community. It is aiming to develop a more agile workforce with innovative technologies like Microsoft Office 365, communication and collaboration tools and giving all staff mobile technology.

Part of that digital strategy is a robust cyber security regime with several technologies in place to ensure citizens, council staff and the services that the council provides are protected. As a result of this layered approach to IT security, council systems are very well protected against known or unknown threats.

But like many other organisations and businesses, Coventry CC has become increasingly concerned about ransomware. This is malicious software, which financially motivated criminals use to attack data.

Once in an organisation's system, ransomware encrypts files so they cannot be accessed. It changes file extensions rather than names, so it is difficult to find corrupted files. Ransomware can infect up to 7,000 files every minute. Criminals then demand payment effectively holding business-critical data and information hostage.

The impact of ransomware was highlighted when another UK local authority was attacked in late February and took two months to recover its data and restore services. An international business hit by ransomware saw its share price plummet and restoration costing millions of pounds. The other issue that spurred Coventry CC into action was the COVID-19 pandemic and the increased vulnerability from the high number of staff working at home.

"The traditional defence against cyberattack is end-point technology like firewalls, antivirus software and network penetration based on prevention rather than focusing on an actual outbreak of encryption. It focuses on stopping anything getting on to your network. But what happens if something does get in? That's the real danger of ransomware. The only way to stop it is a physical lock down. But by the time you do that a lot of damage has been done," says Gary Griffiths, ICT Engagement Lead, Coventry City Council. "The big issue is the time and cost to restore services and it's a growing problem."

Coventry CC discussed the issue with Ricoh, now one of the council's leading strategic partners. In response to the threat, Ricoh has developed a solution to help organisations defend themselves against ransomware. Griffiths says, "In our due diligence research and competitive evaluation of the Ricoh solution we found that there was nothing else like it on the market that delivered such an effective last line of defence. So, it wasn't a difficult decision to choose the Ricoh solution."

Solution

Coventry CC has installed Ricoh's RansomCare solution powered by BullWall ransomware software with support services from Ricoh's Cyber Security Practice. RansomCare is an agentless application that is installed on a virtual server in the council's central IT system instead of every endpoint. It monitors, in real-time, data across the entire enterprise. It can spot a ransomware attack - usually via a laptop or desktop - anywhere across the entire network even when it has managed to by-pass existing security systems. Instantly, RansomCare locks down the location and stops the ransomware from spreading.

A dashboard presents IT with a real-time picture of activity and fires an instant alert if there is an attack. The system automatically provides a detailed attack audit and report for analysis and GDPR-compliance.

The solution started by protecting the council's main data but is now being rolled out to other data such as onsite hosted SharePoint and Office 365 applications. Although not required by Coventry CC, RansomCare can also protect cloud data.

To support the council, the Ricoh service included five days of consultancy covering installation, monitoring and training which was all done remotely. The solution was evaluated, planned, tested and deployed in two months. Software installation was even quicker – just half a day. The BullWall software has been leased from Ricoh under a five-year support plan.

continued overleaf

Benefits

The Ricoh RansomCare solution gives Coventry CC one of the best defences against ransomware currently available on the market. It is quick and easy to install and has minimal impact on IT infrastructure and performance. Compared to the impact on services, business continuity and cost of dealing with a ransomware attack, it represents very good value for money. Even if there is an attack RansomCare stops it instantly before it causes significant damage. It is protecting the data the council uses to deliver services from highways and education to social care and finance.

Griffiths says, "Hopefully, Coventry CC will never suffer a ransomware attack, but Ricoh's RansomCare solution is like an insurance policy. If we didn't do this and had an attack, we'd have to justify why, for the cost of the solution, we could have prevented months of system lock down and millions spent repairing data. Now we have something that should a ransomware attack by-pass our front defence, we have further assurance about how we can manage the impact."

One of the key benefits has been to counter the impact of the COVID-19 lockdown. The council recognised that there was a heightened risk with more staff working from home. Despite robust security systems, the biggest risk to any organisation is user error such as clicking on a link in an email, accessing dangerous websites or inserting an infected USB driver. This increases when people are away from an office and less mindful of security practice.

Griffiths adds, "RansomCare is there to protect the network in case something happens to get in. It may never be used. But with the concerns around the world about the growth of ransomware attacks and cyber criminals getting ever more creative we are doing more than most people to protect the council, its data and the services it delivers."

Ricoh Solution/Products

- RansomCare
- Bullwall software
- Ricoh consultancy and training services

"Hopefully, Coventry CC will never suffer a ransomware attack, but Ricoh's RansomCare solution is like an insurance policy. If we didn't do this and had an attack, we'd have to justify why, for the cost of the solution, we could have prevented months of system lock down and millions spent repairing data. Now we have something that should a ransomware attack by-pass our front defence, we have further assurance about how we can manage the impact."

Gary Griffiths, ICT Engagement Lead, Coventry City Council

Coventry City Council

RICOH
imagine. change.

www.ricoh.co.uk