Lessons learned from Nine's ransomware nightmare

Nine CITO Damian Cronan and group director of IT security Celeste Lowe talk about the cyberattack and what changed at the organisation after.

By David Binning
Associate Editor, CSO
MAY 22, 2022 1:00 PM PDT

In late March 2021, Australia's largest media company Nine was rocked by a major ransomware attack, pushing its head of IT and newly appointed first head of cyber onto a true war footing.

Coming amid a sharp rise in cyberattacks throughout the COVID-19 pandemic, several broadcast and other operations were seriously disrupted, while Nine's shares fell by as much as 2.4% as news got to market.

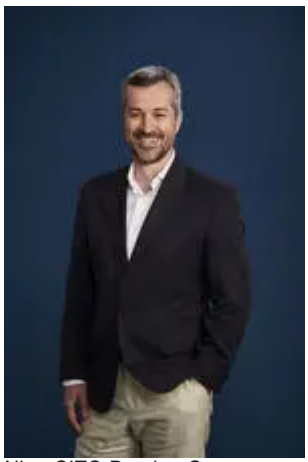
Nine's IT wake up to a ransomware attack

It was 2am on the morning of Sunday March 28 when Damian Cronan, Nine's chief information and technology officer, took the call.

[Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSO newsletters.]

"[I received] a phone call from one of our senior security engineers, who basically advised me that there was every indication from what we were seeing at the moment that there was a major ransomware attack on foot within the night in the business," he tells CSO Australia.

“We didn't yet have a good handle on the extent and scale of it, but it was significant from everything we could see. And from there, obviously, the mind immediately ticks through ‘okay, what do we need to do next?’. We set up a bridge and put a team together and started waking people up basically, and doing what we can, like in any incident response like that, to contain and isolate,” Cronan says.


Nine CITO Damian Cronan

Next on the list was making the call to Nine CEO Mike Sneesby. This was followed by a decision to call the team to work from a single location, the office, and reaching out to Nine’s newly appointed group director of IT security Celeste Lowe to ensure the right cyberresponse.

With the identity and origins of the attacker still unknown, Cronan worked with his team and Lowe to segment and self-contain different areas of the business. This included severing connections between Nine’s broadcast environment and interstate offices, as well as separating corporate networks from publishing networks.

“That was purely an attempt at remediation and containment because we didn't yet know how far and how widespread the threat adversary or the particular ransomware attack had spread,” Cronan says.

Lowe then immediately triggered Nine's 'very significant incident response' process, designed for situations like these. Comprised of two main parts, the first was focussed on business continuity; figuring out what elements were critical to restoring business services. Cronan and Lowe had to work with business teams to answer key questions such as "Can we stay on air?", "Can we get newspapers out?", "Can we collect revenue?" and "Can we pay people?".

The second part involved assessing what competence Nine had against the adversary it was facing and have they been contained and isolated from critical environments.

There was much uncertainty at this point. Lowe and her team had figured out the attacker was using the MedusaLocker ransomware, but still there was no information about the identity or location of the attacker, nor their motivation. There was speculation — since dismissed — at the time that the attackers may have been Russian state sponsored, retaliating against perceived unfavourable reporting about Vladimir Putin in Nine programs and publications.

On the other hand, given that MedusaLocker is an example of so-called ransomware as a service, it could have been anyone, possibly even a child.

Nine works to contain the ransomware attack

Whoever they were and whatever they wanted, the urgent priority was ascertaining whether they were still in the environment. Lowe and her team undertook forensic containment and isolation activities until they were sure the attackers had been repelled.

Nine group director of IT security Celeste Lowe

Formerly a senior cyber analyst with Australian airline Qantas, and before that director of the Cyber Intelligence Centre with Deloitte Australia's risk advisory, Lowe admits — as does Cronan — that she'd never experienced a cyberincident like this before in her career. And being that it occurred at a high-profile media organisation made the challenge of responding ever greater.

“I think that's the uniqueness of working for a media organisation...you’re so much more visible. I suppose it changes your playbooks and how you run an incident and managing information flow, which is always so critical, externally and internally,” Lowe says.

Cronan and Lowe worked together to create what he calls a “war room” of 10 to 15 core engineers, managers and other experts that worked on the recovery from day one and for about three whole months.

“It’s testimony to the team, they all lifted and there were no expectations or people rolling out the door at 5 [pm] we have people working around the clock, in many cases, multiple days. And in some cases, sleeping on site to make sure that that we were able to make ends meet, and a lot of it was extremely collaborative because there is an absence of information early on and there's a lot of decisions that need to be taken,” Cronan says.

For instance, any technology decision needed to be considered in terms of whether it was safe, as well as ensuring they weren’t painting themselves into a corner, and getting things right meant constant face-to-face collaboration. And of course, all of this needed to be communicated to the CEO and the board.

“We took considerable effort in the early days to make sure that the board were up to date, and our CEO, Mike Sneesby was key to that as well, and making sure that flow of information was clear, concise and up to date, in terms of where the board's understanding of the matter was, we also did briefings across the business,” Cronan says.

To Lowe, who had joined Nine only a few months before the cyberattack it was a “baptism of fire”

“There was an enormous amount of trust with all of the stakeholders in the business that they placed back on technology, and Damian and me and the rest of the team to get on and do what we needed to do. I don't think there was any second guessing whether they were the right decisions or wrong decisions,” she says.

Of course, Lowe’s appointment was especially prescient given the attack in March 2021. And Cronan notes that the process of having her position approved and created, and then bringing her onboard created a level of trust that served Nine well when it was so seriously tested just months later.

“The discourse around bringing Celeste into this and our desire to improve our overall security posture certainly helped build a level of trust that preceded the incident,” Cronan says.

What changed at Nine since the ransomware attack

While Cronan says he and Lowe had already put in a lot of work to improve Nine’s cyber posture leading up to the incident, they’ve now adopted a far greater “risk-based” approach to cybersecurity.

“What I would say is that the direction was set insofar as Celeste and myself had a mandate to improve the overall security posture of the Nine group like any large business that's undergone a merger and has evolved over many years. Anything else would be boiling the ocean,” he says.

There was a collection of things that were less than ideal in terms of how the business was operating from a security standpoint but coming under attack brought a lot of positives.

“In many respects, we hadn’t yet been able to get a lot of the actual tangible uplift up and running on the ground [before the attack]. But the scaffolding, the framework was in place and the strategy was in place. So, when the incident occurred, by all means the focus was on tactically ensuring that we can continue to operate and function but once the dust had settled the conversation quickly shifted to how we can accelerate through this now that we understand the plan and we've experienced the consequences,” Cronan says.

For instance, Lowe notes that while Nine had begun implementing the CIS (Centre for Internet Security) framework prior to the incident, the company has since accelerated its deployment to bolster detection, defence and response capabilities.

Several “third parties” that were brought in to work with the war room and broader teams in the first few hours of the attack have been retained to help out with this effort, which has included deploying several off-the-shelf security products.

Moving forward, Lowe stresses the importance of keeping things simple; no mean feat given the complexity presented by the merger of several businesses when Nine bought Fairfax.

“We are focusing strategically on [the] simplification of that. We've gone quite hard...understanding our landscape, the assets within it, and the levels of controls that we need on them. We certainly understand the prioritisation of how our business operates. That is also an opportunity that came out of the incident,” Lowe says.

The incident has helped Nine underscore the critical role that people play in cybersecurity, prompting Lowe to allocate more resources to bolster training programs across Nine. These are a mix of ‘mandated’ and ‘opt-in’ depending on the risk profiles of individual roles, she explains, with some staff required to take part in phishing simulations. General face-to-face as well as one-to-many training sessions have increased, while Nine staff have more opportunities to take part in lunch-and-learn events.

“Obviously, people with privileged access to certain systems need different type of training to those, general [workers] just working in email all day. I think you need to look at your target audience, and what you are trying to get out of it. And what risks you are trying to reduce,” Lowe says.

“Never underestimate the power of people in an organisation as they're a part of your defence layers. [Bringing] as much knowledge in your toolset to educate them and raise that level of awareness, from the most basic to them through to the more complex is absolutely essential,” she says.

Nine defines what is critical in its cybersecurity

A question Lowe and her team now ask themselves is ‘what is business critical to us versus what is cyber critical?’.

“We've prioritised managing some of the security controls specifically and obviously looking at our assets on the edge. And what do we actually have public facing and making sure that they're protected as well as they can be. So, we've taken a very risk-based view of that and really understanding our landscape.”

Cronan says Nine's planning for cybersecurity took into account the nature of media businesses.

"There are some unique aspects to the media industry that make us a particular focus of certain interest groups out there, and as well as the standard run of the mill, criminal threat actors. It's a complex threat landscape for us. And that's also informed our focus and our strategy around how we respond to it."

Cronan says that while media is certainly an increasingly important industry and service that needs to be protected, Nine is yet to be formally approached by Home Affairs regarding the newly passed Critical Infrastructure Bill ."We haven't formulated a view on whether we fall into that bracket," Cronan says although Lowe confirms that "it's under evaluation".

"It means something different to every organisation when you talk about a SASE [secure access service edge] or a zero trust model. And I don't think there's a one size fits all for every organisation and I don't think there's one product out there," Lowe says.

"You've got a lot of vendors that like to tell you either their product is a SASE, or zero trust, but I think for every organisation—as we've done here at Nine—you have to evaluate those components and go with what fits in and what looks right. It's not to be taken or done lightly; it does require a lot of investment. And I think it takes a lot of effort in sustainability. And that's also not often factored in to how much it takes to maintain and run some of them. It's certainly not for set and forget," she says.

Next read this

- *The 10 most powerful cybersecurity companies*
- *7 hot cybersecurity trends (and 2 going cold)*
- *The Apache Log4j vulnerabilities: A timeline*
- *Using the NIST Cybersecurity Framework to address organizational risk*
- *11 penetration testing tools the pros use*

David Binning is an associate editor at CIO Australia.

7 hot cybersecurity trends (and 2 going cold)