



# FAIRVIEW HEALTH SERVICES: TRANSFORMING FROM THE HEART

PROJECT PARTNERS



Jim Brady, VP Information Security & Infrastructure/Operations, and CISO, discusses his dual role at Fairview, the technology transformation the organisation is going through and why people are his biggest asset as an IT leader

**WRITTEN BY DAN BRIGHTMORE & NELL WALKER**

**PRODUCED BY CRAIG DANIELS**



---



# **FAIRVIEW HEALTH SERVICES: TRANSFORMING FROM THE HEART**





A health service that heals from the heart, Fairview Health Services is Minnesota's choice for healthcare - an industry-leading, award-winning, non-profit with 34,000 staff offering a full network of healthcare services and 100+ specialties across 100 hospitals and medical centres.

“Our broad network is designed to be ready for our patients’ every need, while delivering quality care with compassion. Our care portfolio includes community hospitals, academic hospitals, primary and specialty care clinics, senior facilities, facilitated living centres, rehabilitation centres, home health care services, counseling, pharmacies, benefit management services, and the health insurer PreferredOne. We’re built on a tradition of compassionate care. This is our home, and our patients are our neighbors. We’re here to heal, we’re here for you.”

M Health Fairview is a partnership with the University of Minnesota Academic Health Center and University of Minnesota Physicians.

“M Health Fairview started with the idea of putting the latest research in the hands of talented local providers. The results of these collaborations can be summed up in one word: ‘breakthroughs’. Breakthroughs for patients, and breakthroughs for science. So, we decided to expand the partnership. Now we’re bringing the top talents of academic and community medicine even closer so they can bring advanced healthcare from the forefront of medicine to the doorstep of your community.”





**A**n award-winning non-profit organisation, Fairview Health Services is an extensive network of healthcare offerings for hospitals, clinics, senior facilities, pharmacies, rehab centres, and far more, all across Minnesota. In the organisation's own words, Fairview is a 'health service that heals from the heart'. Its goal is to provide compassionate care with its 100 hospitals and care centres, over 100 specialities, and 34,000 employees delivering that care. A noble quest, and one that requires fit-for-purpose IT to support it.

Jim Brady wears two hats within Fairview – VP Information Security & Infrastructure/Operations, and CISO. He began at Fairview as interim CISO and VP, before a CTO-type role in infrastructure also opened up and it was offered to Brady. "A wonderful opportunity!" he responded, already confident after just a few weeks with the IT team that he understood the assignment.

Brady was very comfortable with IT leadership roles already and was quite happy to blend his two positions at Fairview without issue. In fact, spreading his skills across two roles is reflective of one of his first moves within his joint role: to break down silos within Fairview and build increased collaboration.



# Healthcare leaders like Fairview Health Services select Ordr to protect their connected devices



## SEE

every device and network connectivity



## KNOW

every risk, vulnerability and anomaly



## SECURE

with proactive, reactive and retrospective policies

Connected devices including your IoMT devices are critical to patient care, and need to be secured. Get a demo on how we enable real-time asset visibility, identify security and clinical risks, and implement Zero Trust security for the top healthcare organizations in the world.



Request a demo at [www.ordr.net](http://www.ordr.net) or email [info@ordr.net](mailto:info@ordr.net)

---

**“WE’RE MOVING TO THE CLOUD  
BECAUSE WE WANT OUR PATIENTS –  
OUR CUSTOMERS – TO EXPERIENCE  
ALL THE BENEFITS THAT A TYPICAL  
CONSUMER WOULD GET”**

**Jim Brady**

VP Information Security &  
Infrastructure/Operations, and CISO

### **BREAKING DOWN SILOS**

“There were some silos for a number of years between security and infrastructure, because they fell under different leaders and sometimes there were competing agendas and budgets,” Brady explains. “Having all of it under one umbrella was helpful to bring those leaders and teams together into more of a collaborative partnership. We’re now all rowing the boat in the same direction and supportive of the group goals.”

The second thing Brady did to merge IT into one supergroup was give everybody a security role within the infrastructure group. Security is a vital area of IT, an organisational imperative, and having everyone understand that – and the reasons why – has made an enormous difference compared to leaving security purely to the security team.

“As we began to spend more time together

planning, partnering, and problem-solving, I soon started to see people work closely, collaboratively,” says Brady. “It definitely helped us. Oftentimes, one leader would pitch in and help with something that maybe wasn’t their area. When you see that happening, you know you’re functioning well as a team.”

### **PEOPLE BRING PROGRESS**

Given his passion for collaboration, it’s no surprise that Brady is a person who’s driven by helping people. While he considers himself something of an introvert, he can be extroverted when it comes to leadership and describes himself as having a Type A personality - high-achieving and motivated, excellence-driven and, more importantly, mission-driven.

“I spent the first part of my career working in a faith-based non-profit organisation, and





# Transform the future of health with AWS

Healthcare and life science organizations are reinventing how they collaborate, make data driven clinical and operational decisions, enable precision medicine, and decrease the cost of care. Amazon Web Services (AWS) is dedicated to a world where every person has the opportunity to live a life of dignity on a healthy planet.

Whether you are working to improve healthcare systems, the performance of donor-facing websites, enhancing data analysis, propelling research through machine learning, or improving remote monitoring with the Internet of Things (IoT), AWS is here to help. Tens of thousands of nonprofits and non-governmental organizations worldwide use AWS to increase their impact and advance mission goals.



**Get started with  
resources curated  
for AWS Public Sector  
Healthcare customers**





I found that when I shifted to healthcare, it's an industry that people don't choose to work in to primarily make money or climb the career ladder – there's always a bigger reason," says Brady. "I love people, helping them and interacting with them in a positive way. There are several hundred people on my team, but I still spend time with them one-on-one and in small groups, even now that we're largely working remotely."

Being close with his blended team has ensured Brady can really push continuous improvement within the IT department of Fairview Health Services. Change is constant when it comes to technology, but professionals in that sphere are used to the pace. "We're changing to be more digital," says Brady, "We're moving to the cloud because we want our patients - our customers - to experience all the benefits that a typical consumer would get."

For Brady and his team, it's not just about providing patients with what they need but making sure the entire experience is an excellent one. If that can't be delivered due to a ransomware event or other security problem, that's an issue. And while the majority of people working in IT aren't interacting with the end-user, Brady is always there to remind his team of their purpose.

"Not knowing how what you do is impacting patients on a tangible basis can cause people to forget why they're working, but we're a mission-driven entity. It's important that we always understand what we're doing from a business perspective. I've had roles in the past where we would bring IT staff to hospitals or clinics and have them walk around and see what life is like for the front-line people working there for a couple of hours, so they understand how important their work is."

## A SECURE TRANSFORMATION

With his blended team in place and focused on a higher purpose, Brady has been able to guide Fairview through its IT transformation effectively. The organisation began investing in cybersecurity before Brady joined the team and some great progress was made, but much more needed to be done due to the rapid increase in extortion events, ransomware, and the general growing threat landscape. A few years ago, healthcare wasn't a particularly targeted sector by cybercriminals, but it's become a critical issue.

"It's unthinkable that people would go after Acute Care and Paediatric hospitals to shut down medical devices, but that's what's happening because cyber-crime is a lucrative business," Brady explains. "They're not feeling the pain and suffering they're causing. When you shut down a health system for three-to-four weeks, patients are harmed, and life-threatening illnesses and injuries are not prevented. So, it's not just about fines and data breaches for us - this is people's lives."

This rapid increase in risk means that departments like the one Brady oversees have to do something different. Fortunately for him, Fairview's senior management and its board of directors agree, and are continuing to actively invest in cybersecurity to build and solidify the foundational technical controls.

"What we've done at Fairview is ask,



'What can we do? Where are we in need?' says Brady. "We were short-staffed, some of the security engineers' job roles were outdated. We took steps to make ourselves a more attractive employer with competitive salaries and modernised job classifications. It's tough to hire security experts, and we struggle to compete with tech companies, but what we can offer is a mission-driven purpose with market competitive compensation. With the right people in place, we've worked hard to revamp and





transform the security structure we've got."

And fortunately, there's a roadmap for Fairview to follow. Healthcare organisations are required by HIPAA to conduct ongoing risk assessments, and this gives Fairview the blueprint of what it needs to work on when it comes to technology. "It allows us to identify and close any gaps there might be," says Brady. "We don't have unlimited funding, so we prioritise based on the top risk areas. That also helps us think smarter about improving the organisation."

## **FUTURE READY HEALTHCARE**

Brady is more aware than most that the healthcare sector has a reputation of being 20 or even 30 years behind when it comes to technology. Consumer industries, manufacturing, finance – they are all far more streamlined and moved to the cloud ahead of healthcare. Wearing his IT and infrastructure hat, Brady was and is determined to change this for Fairview.

"There was a concern, in healthcare, that our data couldn't be put into the cloud





**FRSECURE**<sup>®</sup>

**PROVIDING  
CYBERSECURITY  
SOLUTIONS  
THAT MAKE A  
MEASURABLE  
DIFFERENCE**



**FRSECURE.COM**



**(866) 302-1167**

**Stay One Step**

**AHEAD**

**With Continuous Cybersecurity Support**

As the world becomes increasingly digital, the attack surface grows. Stay one step ahead with complete cybersecurity programs that drive resilience and accelerate business progress. At Optiv, we manage cyber risk so you can secure your full potential.



[www.optiv.com](http://www.optiv.com)

**Secure greatness<sup>™</sup>**

because of HIPAA regulatory and security concerns,” he says, “but it’s been proven that the cloud is as secure - if not more so - than on-prem data storage.” Healthcare isn’t a sector where many of its IT solutions are built in-house, and most health systems don’t have large in-house application development teams.

“We might not be able to move to the cloud as aggressively as other industries, but we do have an initiative I’ve been working on where we’re moving around 40% of our infrastructure to the cloud,” adds Brady. The additional security offered by cloud storage means that Fairview can start fresh with more mature security controls in a new cloud infrastructure, thus reducing the cyber risk that is often found with the technical debt in legacy on-prem compute and storage. Business interruption for a large healthcare network is a real concern, and Fairview can’t afford to risk lives, lose data, or have to pay out millions of dollars in ransoms or fines.

“While we can’t stop cyberattacks from happening, we can now emphasise timely detection,” Brady states. “So many organisations will put their focus into firewalls, antivirus protection, and other protective and reactive security controls. We recently started to track the statistics of how many cyberattacks happen through email, through the network, through firewalls and through web browsing. It’s not uncommon for Chief Information Officers

**“IT’S UNTHINKABLE THAT PEOPLE WOULD GO AFTER ACUTE CARE AND PAEDIATRIC HOSPITALS TO SHUT DOWN MEDICAL DEVICES, BUT THAT’S WHAT’S HAPPENING BECAUSE CYBER-CRIME IS A LUCRATIVE BUSINESS”**

**Jim Brady**

VP Information Security  
& Infrastructure/  
Operations, and CISO

to have a key metric involving five 9’s of availability. In cybersecurity, we don’t have this type of well adopted metric. Measuring the number of cyber-attacks can be useful to raise awareness to the level of cyber risk an organisation is facing. It was quite shocking to realise that attempted attacks don’t happen just a handful of times a week – we’re averaging 650,000 attacks every day. And we’re only a medium-sized healthcare organisation. It’s not always possible to block all of those attacks, but timely detection is important in informing the layered defences you put in place.”

## PARTNERSHIPS

The partnerships Fairview has formed have been a key element of its technology transformation. Continuing the topic of threat detection, this was an area where Fairview didn't previously have an enterprise threat detection solution in place, but it quickly came to realise threat detection is vital. This is where Gigamon stepped in.

"We looked at various providers in this area and Gigamon impressed us the most," says Brady. "They've identified a number of anomalous activities that we've been able to address quickly; without that, we wouldn't know who's in our back yard. We wouldn't be able to detect it without them because there are simply too many alerts coming through the logs for any human to understand it, so that's been incredibly helpful."

With Optiv, another of Fairview's partners, the support has been on the value-added reseller side. "They've helped us understand what products and services would be good for us to consider," Brady

explains. "Having a neutral third party that can work with multiple products and vendors is helpful, rather than only deal directly with the vendor. They've also been negotiating prices for us, so I've found value with Optiv."

Fairview's biggest risk area is in the medical devices space, so it has Ordr on board to uncover any IoT problems. "We have over 130,000 devices that Ordr can identify the vulnerabilities and risks of. That gives us a head start on closing those vulnerabilities. Threats are changing by the day but the vendors of medical devices don't offer much guidance. However, Ordr tracks vulnerabilities, identifies what is and isn't normal activity and addresses any issues. Ordr has been great to work with... When I first stepped into my role Fairview had bought the product but not fully deployed it because we didn't have the right staffing. Ordr stepped up and helped us."

Fairview has its own internal incident response team, but it still needs external forensic support depending

on what the incident is - so FRSecure (a local Minnesota company) was brought on board. "They've been great," says Brady. "We call them in for forensics services on post-incident analysis whenever we need it. They're very responsive and provide personalised support."

To fully leverage the benefits of cloud Fairview calls on AWS (Amazon Web Services). "AWS is a customer obsessed and very responsive organisation - the market leader in the cloud business," notes Brady. "We were looking to move off our on-prem contact centre, so we reached out to them and talked about using what they had initially developed as their own contact centre and interactive voice response (IVR) system centre. It is a great product called Amazon Connect, and we're in the process of moving our on-prem contact centre to it. I've been very impressed with how customer-focused AWS is, and their philosophy is to teach the customer how to fish rather than doing all the fishing for them, which is very empowering."







**“THE REASON FOR OUR EXISTENCE IS TO PROVIDE PATIENT CARE, SO WE HAVE TO ENSURE THAT THE RIGHT FUNCTIONALITY IS THERE TO SUPPORT THEM”**

**Jim Brady**

VP Information Security  
& Infrastructure/  
Operations, and CISO

## OVERCOMING CHALLENGES

No transformation comes without challenges. Brady learned the hard way that focusing IT efforts on a few priority projects rather than trying to support too many projects at once is far more efficient and successful – and this is undoubtedly true across many industries – which the COVID-19 pandemic highlighted. “With the pandemic, we had to shift pretty quickly to working on what was the biggest priority based on the fact that staff had to go remote,” Brady explains. “It was such a crisis that we had to really focus on supporting the digital side of remote work and doing what we could to handle the many, many COVID patients we were seeing. Fortunately, just

**Your network is in the cloud, but that doesn't mean your head has to be.**

Without deep observability, you're exposed.

**Gigamon®**

Get deep observability  
[gigamon.com/deep-observability](https://gigamon.com/deep-observability)





a couple of months before the pandemic hit, we had moved over to a cloud-based remote access system, which helped tremendously.”

Internet bandwidth also had to be increased to support remote staff, and while telehealth wasn’t largely adopted prior to COVID-19, it ramped up once it took the world by storm. “There was a lack of adoption in certain specialties, certain areas, certain doctors – but it became the only way you could see patients, so we ended up having several telehealth solutions.”

With remote working becoming the norm, security once again became a talking point within Fairview. The organisation already had a policy in place that workers had to use a company device to access company

applications and data; using a cloud-based private network for remote access added a layer of security. There were challenges here as well, since not everybody had a company device, so Brady and his team created a second method of access through personal devices via a web-based gateway with secured access.

“One thing we did was make sure there wasn’t a open remote desktop protocol (RDP) – where people can access their work computer from a personal computer,” says Brady. “We don’t know what people are running on their home network and what their security level is, so that was too risky. But for the most part, we didn’t experience any significant remote access issues caused by the pandemic on the security side.”



## WHAT'S NEXT?

All of the changes Brady has made, and the way he's reshaped and guided his team through several uncertain years, have undoubtedly been wildly successful. So much of this is down to his faith in people. "I think people are the key to a successful organisation," he says. "Successful companies and CEOs are always pointing to the fact that their most valuable asset is people."

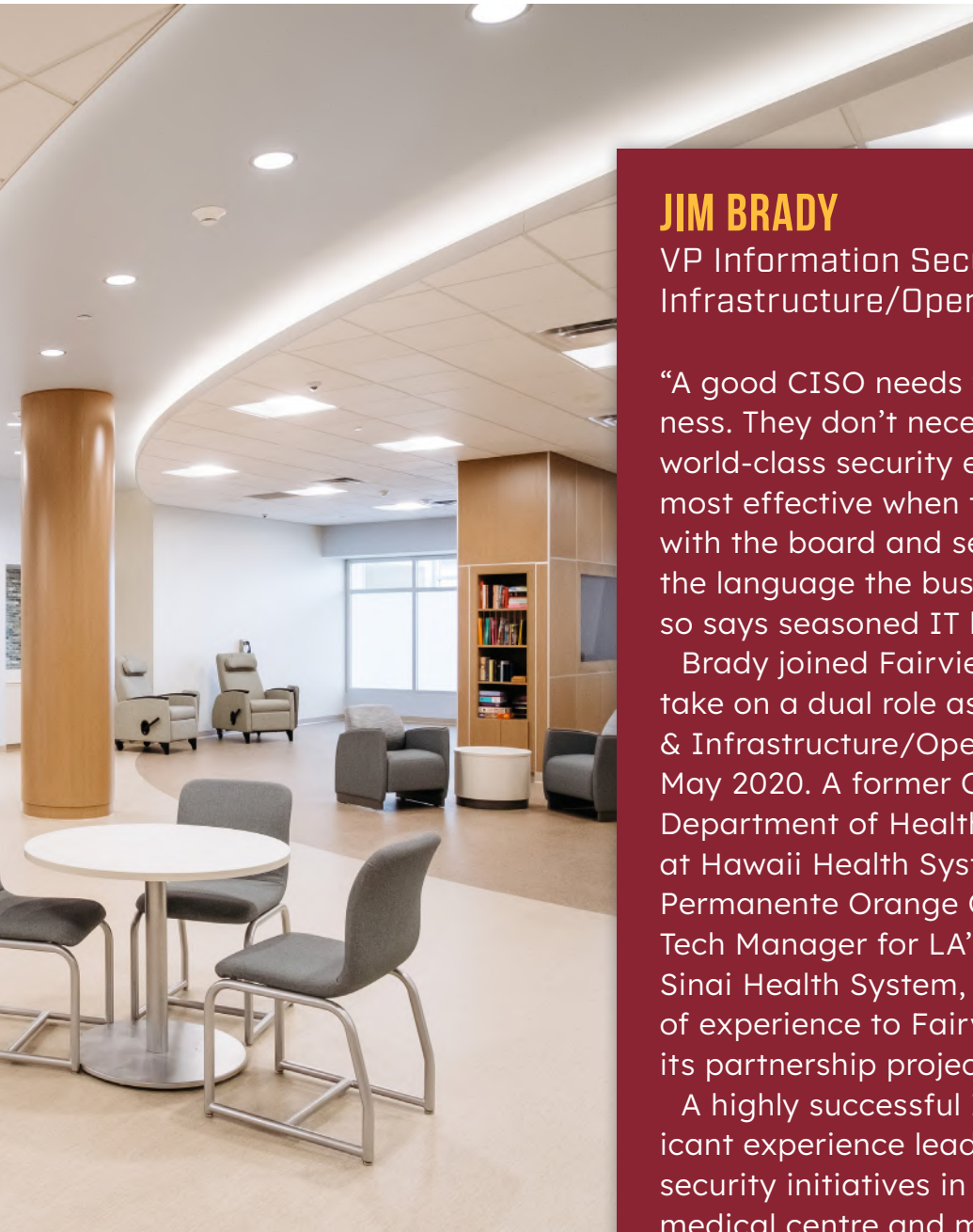
Most importantly, Brady truly understands IT and Fairview's needs - which bodes well for the organisation as it continues to evolve. "In addition to fortifying our foundational security posture, we've expanded our threat detection considerably," he continues. "Plus, as an organisation, we have committed to providing digital services to our patients and customers. That means embracing the cloud and expanding our on-prem environment to both the data analytics side and the foundational, diverse virtual services side.

"We're also looking to modernise our teams by further leveraging remote work and utilising a global workforce. One never-ending battle for me is educating our workforce on appropriate security culture, and we're seeing great results there. We also still have a lot of legacy infrastructure and we're continuing to drive virtual care forward to combat that. We're future-proofing Fairview with the cloud and constantly improving customer



engagement. The reason for our existence is to provide patient care, so we have to ensure the right functionality is there to support them and that risks to their care are eliminated in a timely manner. It's truly what drives us and inspires us." ■





## JIM BRADY

VP Information Security & Infrastructure/Operations, and CISO

“A good CISO needs to understand the business. They don’t necessarily have to be a world-class security engineer, but they’re most effective when they communicate with the board and senior management in the language the business understands,” so says seasoned IT leader Jim Brady.

Brady joined Fairview Health Services to take on a dual role as VP Information Security & Infrastructure/Operations, and CISO in May 2020. A former CIO for LA County’s Department of Health Services, CISO & CTO at Hawaii Health Systems, CIO at Kaiser Permanente Orange County in California and Tech Manager for LA’s world-renowned Cedars Sinai Health System, Brady brings decades of experience to Fairview in Minnesota and its partnership project M Health Fairview.

A highly successful IT executive with significant experience leading technology and security initiatives in complex academic medical centre and multi-hospital healthcare settings, Brady strives to be a committed, transparent and strategic thinker. He has a track record of quality, systematic decision making, providing transformational and business-focused value in the new digital age.

“Understanding how our organisation generates revenue, what its key drivers are, what’s important for the future – this is vital,” adds Brady. “Balancing that with ensuring the continuity of treatment for our patients, informs my priorities as CISO.”

