

The University of Manchester strengthens cybersecurity by partnering with Tanium

After a phishing attack, a new security strategy features Tanium plus third-party suppliers.



ORGANIZATION

The University of Manchester

LOCATION

Manchester, England

It's every organisation's cybersecurity nightmare: Bring in their first ever CISO then suffer a crippling cyberattack just five weeks later.

For The University of Manchester, it was a reality. In May of 2023 the university suffered a serious phishing attack. The attackers gained access to the university's network, elevated their privileges, and then copied proprietary data.

"I got that phone call that every CIO absolutely hates to get," recounts university CIO Patrick "PJ" Hemmaway. "Which is, 'We think we've got a breach.'"

To counter the cyberattack and limit the damage, Hemmaway and his team quickly shut down many IT services. Once a sufficient amount of time had passed, they began what the university calls the restoration and stabilisation phases. First, all shut-down services were restored. Then the platform was stabilised, largely with updated patching.

It was a difficult period. A full year after the attack, Hemmaway says, "We've still got a little bit of PTSD."

A collective effort

The University of Manchester has now entered what CIO Hemmaway calls the improvement phase. This has included adding two divisions to the IT services staff, bringing the total to seven divisions. The university has also established a new security strategy that focuses on five primary goals:

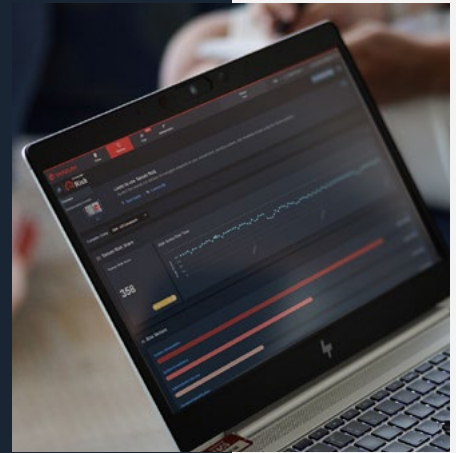
1. Maintain security by ensuring continued security of the university
2. Deal with security debt by increasing capacity and capability
3. Increase maturity by delivering increased operational efficiency
4. Ensure confidence with stakeholders
5. Continuously improve by continually reviewing the risk posture

To help achieve these goals, the university's security strategy now features working with partners. One of those partners is Tanium. Alex Goffe who joined the university shortly after the attack as its new director of campus technology services, had learned about Tanium in a previous job. Once at Manchester, Goffe realized the university's team needed a tool that could provide full visibility into endpoints across the entire network. He suggested they talk with Tanium.

"With Tanium," Goffe says, "the ability to see all this information in a single application is really powerful."

The university opted to work with Tanium, as well as Microsoft and ServiceNow. "These partners," says CIO Hemmaway, "are helping us stay at the forefront of technology and address tomorrow's needs."

Even better for the university team, Tanium integrates well with these other tools. That helps the university avoid what Goffe calls "tooling sprawl." Partner integration, he adds, "just saves a lot of time."





Faster patching

Tanium is now helping Hemmaway and his team populate their new ServiceNow configuration management database (CMDB), giving the university real-time information about their network and endpoints. Tanium is also being used to manage the university's roughly 40,000 endpoints.

While securing a large network doesn't come cheap – in 2023 The University of Manchester heavily invested its cyber incident-related spending – the investment is starting to pay off. Earlier this year, the university received recognition from the UK government for security under Cyber Essentials, a government scheme to protect organisations against cyberattacks. In addition, the UK National Cybersecurity Centre, which provides security advice and support, has recognized The University of Manchester as an academic center of excellence for cybersecurity research.

Looking ahead, the university's cyber team has ambitious plans. One effort will adapt legacy data, so that it can be interrogated by AI systems.

Another future effort will aim to strengthen the ability of university researchers to share their data with colleagues outside the university – safely, securely, and relatively easily. "Our researchers are constantly asking us to share data," CIO Hemmaway says.

Yet another new project is designed to offer cybersecurity as a commodity service. Under this plan, cybersecurity will be offered like a utility. "It doesn't impact our users," Hemmaway says. "It's seamless."

Taken together, these partnerships and plans are preparing The University of Manchester for the future, including the possibility of more cyberattacks. "I know something will happen, but I don't know what the scale will be," Hemmaway says. "It's my job to make sure we're protected as best as we can be."

"By combining the strengths of Tanium with ServiceNow and Microsoft, we now have a single strategic platform that allows us to have a complete and accurate CMDB with real-time data along with enhanced threat detection and response capabilities that significantly increases our security posture."

PJ Hemmaway
Chief Information Officer
The University of Manchester

Results

Partner power

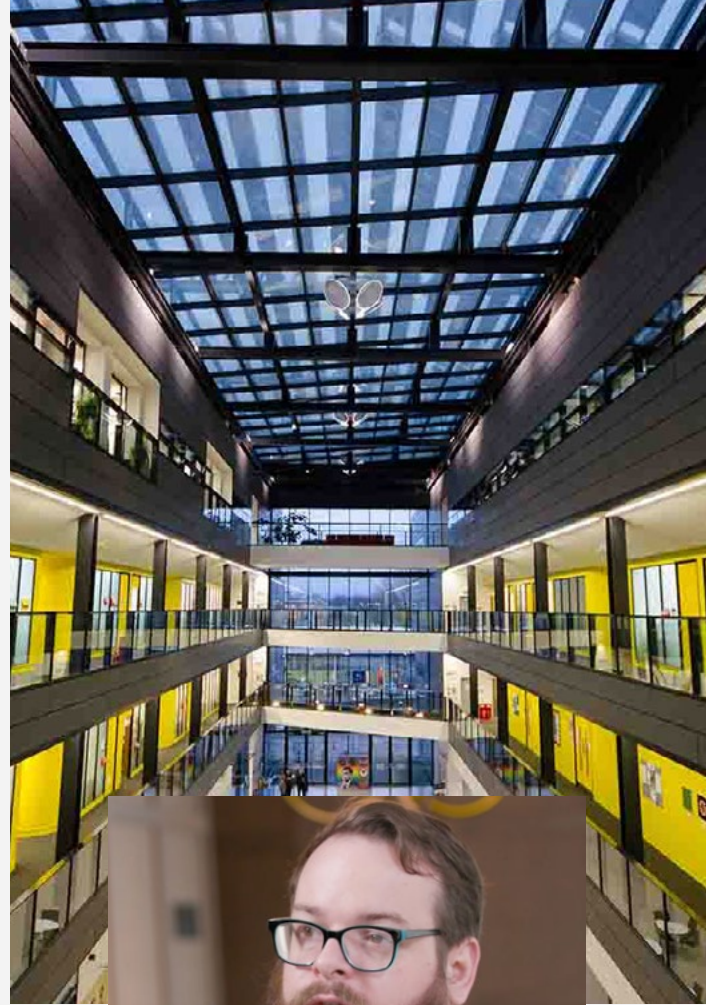
Following a cyber breach, the university is strengthening its cybersecurity by working with Tanium and partners like Microsoft and ServiceNow.

Great integration

Because Tanium integrates easily with ServiceNow and Microsoft, the university avoids what Alex Goffe, director of campus technology services, calls “sprawl.” These integrations, he says, “saves a lot of time and money.”

Royal recognition

The university’s new cybersecurity strategy has won it recognition from two government groups: the UK government, which recognized the university for security under Cyber Essentials; and the UK National Cybersecurity Centre, which named the university an academic center of excellence for cybersecurity.



“With Tanium, the ability to see all this information in a single application is really powerful.”

Alex Goffe

Director, Campus Technology Services
The University of Manchester

Tanium delivers the industry's only true real-time cloud-based endpoint management and security offering. Its converged endpoint management (XEM) platform is real-time, seamless, and autonomous, allowing security-conscious organizations to break down silos and reduce complexity, cost, and risk. Securing more than 32M endpoints around the world, Tanium's customers include more than 40% of the Fortune 100, 7 of the top 10 U.S. retailers, 8 of the top 10 U.S. commercial banks, all 6 branches of the U.S. military, and MODs and DODs around the world. It also partners with the world's biggest technology companies, system integrators, and managed service providers to help customers realize the full potential of their IT investments. Tanium has been named to the Forbes Cloud 100 list for eight consecutive years and ranks on the Fortune 100 Best Companies to Work For.

