NTT DATA

Thermo Fisher SCIENTIFIC

Thermo-Fisher Scientific: a great case for converging IT ops and security

In the early days of business computing, protecting the limited information housed on machines was little more than an afterthought, and mostly a matter of physical security (locked doors, fire suppression, etc.). But over the last 25 years, as nearly every aspect of our personal and professional lives has become digitized and networked, the potential ramifications of data breaches have grown increasingly grave, making robust cyber-security an essential component of every organization. So much so, that many large enterprises have created entire departments of technology experts focused solely on thwarting cyber-security threats.

Security is mission-critical, of course, so a devoted security team still makes sense. But there are downsides to having too much separation between security and the IT operations staff who support employees' everyday computing needs. In a nutshell, isolating security as its own column on the org chart tends to inflate bureaucracy (the enemy of agility) and create conflicts between IT counterparts.

Today, as advanced technology and constant connectedness are keys to success for every business function, it's more important than ever that IT ops and security are on the same page. The effects of the COVID-19 pandemic only strengthen the need for collaboration, as work-from-home employees are now more dependent than ever on seamless network access, online interactions with colleagues, and the cloud-based tools and systems they use daily. As a result, a growing trend among many CIO organizations is to reconsider the working relationship between IT ops and security, and build bridges to bring the two into closer alignment.

Turning conflict into collaboration

An excellent example of this paradigm shift can be found at Thermo Fisher Scientific, a global provider of laboratory equipment and software for the healthcare and life sciences industries, and an NTT DATA client. Bryan Inagaki's latest title at Thermo Fisher – Senior Director of Secure Digital Workplace – speaks volumes, as it captures the increasingly integrated nature of IT ops (workplace) and security. Bryan shared his thoughts with us on why moving in this new direction was right for him and his team.

"We still have a separate security engineering team, but today every element of what we do for the workplace has a security piece built into it. So we're set up to work in close collaboration with fewer barriers between us," says Bryan. "Security is not just a stakeholder in workplace processes, they're viewed as part of the team."

It sounds simple, but this type of partnership isn't typical of most IT organizations. When security exists in its own silo, it often fosters an "us vs. them" mindset. That is, the workplace team wants to create intuitive, frictionless experiences for employees, while security is unfairly seen as the technology killjoy intent on making everything more difficult. Changing the org structure to create shared goals and responsibilities can help transform the overall IT mindset to one of “secure enablement,” approaching every project with equal and simultaneous concern for security and usability.

Benefits on both sides

More than an abstract cultural enhancement, an emphasis on aligning security and IT ops can lead to real-world, tangible results. First off, it creates greater visibility of the organization’s holistic IT needs and challenges, so they can be addressed more efficiently.

When COVID struck in March 2020, for example, Thermo Fisher Scientific’s IT group had already taken steps toward convergence.

“We didn’t make the change because of COVID, but the fact that it was already in motion allowed us to make quick decisions to keep the business running smoothly when everyone went virtual,” said Bryan. “That included things like managing increased network pressure, device management, authentication, etc. Everything ran through one organization instead of having two or three different departments involved.”

The simplified structure led to increased speed and agility as many of the formalities of bureaucracy were removed.

“When it comes to workplace and security collaborating on issues, instead of going ‘up and over,’ navigating the traditional approval channels, we’re free to go ‘straight across’ the org chart and get things done fast,” said Bryan.

As a result, security becomes more seamlessly integrated throughout the technology ecosystem, and has an earlier say in how user options and privileges are vetted and controlled. At the same time, employees benefit from an improved user experience as IT can roll out new services in less time, with security baked in rather than slapped on top.

As a side note, Bryan added that the converged approach has also helped Thermo Fisher’s IT group cut costs and generally achieve a cleaner IT service stack. By converging some systems and tools and removing redundancies, they’ve achieved a stronger negotiating position with technology vendors as they look to the future.

Keys to success

IT issues rarely occur in a vacuum, and every part of the technology organization has a role to play in the secure and effective delivery of IT services. So the first step in bringing security and operations together may be simply recognizing that shared responsibility. Bryan said a big part of Thermo Fisher’s success was based on building trust between IT groups that were often at odds in the past.

Clear and consistent communication was also critical, he said.

“IT tends to be bad at explaining things,” Bryan said. “So we’ve worked hard to really clarify the value of our approach, both to create buy-in among leadership and to communicate with end users.”

To that point, Bryan’s team leverages internal marketing and creative pros to ensure they tell their story clearly and convey the benefits effectively in presentations and communications.

Finally, IT has to embrace the customer service mindset, he said. Everyone in the business depends on technology to do their jobs, thus they depend on IT to make sure technology works as it should. IT groups must be able to set aside their need for total control and make serving their joint customers the top priority. In this case, customer service means partnering with business units and employees to deliver IT solutions that are equally useful and secure.

Whether it’s two distinct IT teams determined to work in closer dotted-line collaboration (more likely for large enterprises), or an official blending of the org chart, there’s value in rethinking the way IT works. That would be true under any conditions but may warrant more urgency given the events of the past year. In a time when businesses need IT more than ever, they need their best IT people working as one, cohesive force for the good of all employees.