

When Heroism Means Staying Out of the News

When Heroism Means Staying Out of the News

Published 9/16/2024 · 3 min read



EUTO Workstation Team's calibrated, collaborated response to the CrowdStrike incident kept Disney parks and properties operational while much of the rest of the world faced blue screen of death shutdowns

On July 19, 2024, CrowdStrike's faulty software update caused widespread problems with Microsoft Windows. Roughly 8.5 million systems crashed around the world — airlines and airports on nearly every continent were disrupted, as were hospitals and health care, banks and financial service companies, media and communications, government and other sectors. It was all over the news, all over the globe. *The Guardian* labeled this event, "largest outage in the history of information technology"

There were no news stories about disruptions at Disney properties. Not because Disney wasn't impacted by the outage, but because of the rapid response and mobilization of the EUTO Workstations Team and on-the-ground field support.

When the issue first became known, just after midnight on the East Coast, the team jumped into action. They quickly realized that to resolve the issue and to keep Disney's parks and financial operations running, someone would have to touch each and every device that had been impacted by the faulty CrowdStrike patch — over 20,000 within Enterprise Technology in the United States alone! And it took approximately 30 minutes to fix each device.

They worked closely and tirelessly with on-the-ground support teams around the world and their efforts succeeded in keeping Disney properties open and operating. By prioritizing guest-facing services and devices, they restored operations in critical points to allow employees to begin their workdays at the North American parks on July 19, as usual, with costumes and uniforms, and to allow guests to enter and enjoy park experiences while the rest of the world was still staring at frozen blank blue screens.

It ultimately took a full week and 1,800 field team remediation manhours to complete the restoration effort. And because even redundant services and devices were impacted, the team had to develop and implement strategy quickly to identify which services to target, in what order. They quickly set up a bridge for emergency communications.

Communications were absolutely vital, particularly when there was no single, one-size-fits-all solution to the problem — rather, the fixes varied by device model and type. All hands were on deck, coordinating seamlessly to handle sudden worldwide issues that encompassed infrastructure, Active Directory, domain controllers, virtual machines. The IT Help desk played a vital role. It also helped that guests as well as employees knew that none of this was Disney's fault and that they granted the company both gratitude for the rapid response efforts, as well as grace in accepting longer wait times, potentially fewer functions (like pictures on park rides).

As the EUTO Workstations Team reflects on that intensely busy week in July that felt (to them) more like a year, they identify the vital importance of communications in all of their efforts, in particular the communications bridge which allowed them to share information quickly and effectively. They also take away the lesson that creating and maintaining good documentation of processes, for each model of device, is vital to supporting these efforts, and to providing a blueprint for others during future emergencies.

Full Text:

EUTO Workstation Team's calibrated, collaborated response to the CrowdStrike incident kept Disney parks and properties operational while much of the rest of the world faced blue screen of death shutdowns.

On July 19, 2024, CrowdStrike's faulty software update caused widespread problems with Microsoft Windows. Roughly 8.5 million systems crashed around the world — airlines and airports on nearly every continent were disrupted, as were hospitals and health care, banks and financial service companies, media and communications, government and other sectors. It was all over the news, all over the globe. *The Guardian* labeled this event the "largest outage in the history of information technology."

There were no news stories about disruptions at Disney properties. Not because Disney wasn't impacted by the outage, but because of the rapid response and mobilization of the EUTO Workstations Team and on-the-ground field support.

When the issue first became known, just after midnight on the East Coast, the team jumped into action. They quickly realized that to resolve the issue and to keep Disney's parks and financial operations running, someone would have to touch each and every device that had been impacted by the faulty CrowdStrike patch — over 20,000 within Enterprise Technology in the United States alone. And it took approximately 30 minutes to fix each device.

They worked closely and tirelessly with on-the-ground support teams around the world, and their efforts succeeded in keeping Disney properties open and operating. By prioritizing guest-facing services and devices, they restored operations in critical points to allow employees to begin their workdays at the North American parks on July 19, as usual, with costumes and uniforms, and to allow guests to enter and enjoy park experiences while the rest of the world was still staring at frozen blank blue screens.

It ultimately took a full week and 1,800 field team remediation manhours to complete the restoration effort. And because even redundant services and devices were impacted, the team had to develop and implement strategy quickly to identify which services to target, in what order. They quickly set up a bridge for emergency communications.

Communications were absolutely vital, particularly when there was no single, one-size-fits-all solution to the problem — rather, the fixes varied by device model and type. All hands were on deck, coordinating seamlessly to handle sudden worldwide issues that encompassed infrastructure, Active Directory, domain controllers, virtual machines. The IT Help desk played a vital role. It also helped that guests as well as employees knew that none of this was Disney's fault and that they granted the company both gratitude for the rapid response efforts, as well as grace in accepting longer wait times, potentially fewer functions (like pictures on park rides).

As the EUTO Workstations Team reflects on that intensely busy week in July that felt (to them) more like a year, they identify the vital importance of communications in all of their efforts, in particular the communications bridge which allowed them to share information quickly and effectively. They also take away the lesson that creating and maintaining good documentation of processes, for each model of device, is vital to supporting these efforts, and to providing a blueprint for others during future emergencies.

Evolution not Revolution

Published 7/1/2025 · 1 min read



Decoding the two recent Notices of Decision (NOD) and what it means practically for you

On June 6, 2025, Global Information Security (GIS) issued two new [Notices of Decision](#) (NODs) which will become policy as of July 6, 2025:

1. [Information Classification](#)
2. [Technical Security Assessment Standards](#)

Both of these policy changes shift the scope in their respective areas. The following is a very high level summary of the changes and what they might mean practically.

1. Information Classification:

- Provides many varied examples of types of "confidential information"
- Exempts systems which, aside from storing secrets are otherwise not considered to be high impact from having to undergo the more frequent cadence of assessments that are required for high impact systems.

Further guidance:

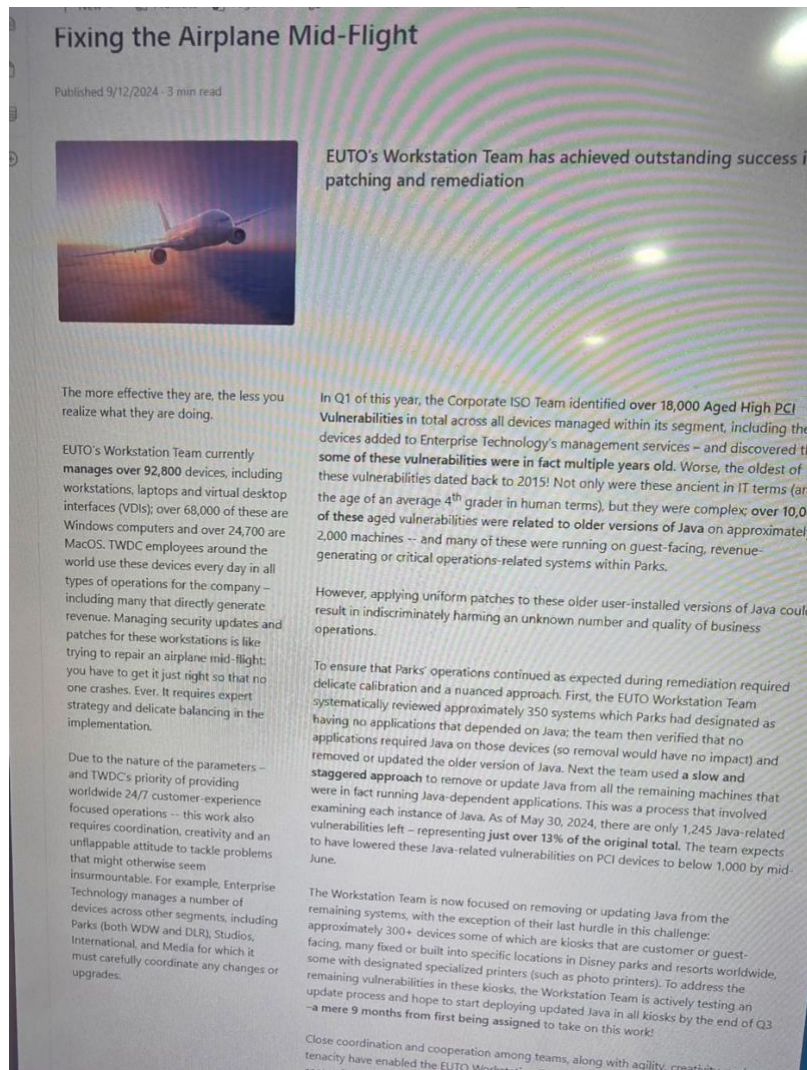
- [FAQ: Where to store and how to securely send confidential information at TWDC](#)
- [Overview of information classification as it relates to ISPS](#)

2. Technical Security Assessment (TSA) Standards:

- Changes the scope and level of automation that TSA testing MAY take (increasing or decreasing automation/manual, depending on the underlying system)
- Does **NOT** change the requirement for which systems must undergo TSA testing

Further guidance:

- [Overview of Security Assessment controls in ISPS](#)



Published 9/12/2024 · 3 min read

Full Text:

Fixing the Airplane Mid-Flight

EUTO's Workstation Team has achieved outstanding success in patching and remediation.

The more effective they are, the less you realize what they are doing.

EUTO's Workstation Team currently manages over **92,800 devices**, including workstations, laptops, and virtual desktop interfaces (VDIs); over 68,000 of these are Windows computers and over 24,700 are MacOS. TWDC employees around the world use these devices every day in all types of operations for the company — including many that directly generate revenue. Managing security updates and patches for these workstations is like trying to repair an airplane mid-flight:

you have to get it just right so that no one crashes. Ever. It requires expert strategy and delicate balancing in the implementation.

Due to the nature of the parameters — and TWDC's priority of providing worldwide 24/7 customer-experience focused operations — this work also requires coordination, creativity, and an unflappable attitude to tackle problems that might otherwise seem insurmountable. For example, Enterprise Technology manages a number of devices across other segments, including Parks (both WDW and DLR), Studios, International, and Media, for which it must carefully coordinate any changes or upgrades.

In Q1 of this year, the Corporate ISO Team identified **over 18,000 Aged High PCI Vulnerabilities** in total across all devices managed within its segment, including the devices added to Enterprise Technology's management services — and discovered that some of these vulnerabilities were in fact multiple years old. Worse, the oldest of these vulnerabilities dated back to 2015. Not only were these ancient in IT terms (and the age of an average 4th grader in human terms), but they were complex: **over 10,000 of these aged vulnerabilities were related to older versions of Java** on approximately 2,000 machines — and many of these were running on guest-facing, revenue-generating, or critical operations-related systems within Parks.

However, applying uniform patches to these older user-installed versions of Java could result in indiscriminately harming an unknown number and quality of business operations.

To ensure that Parks' operations continued as expected during remediation required delicate calibration and a nuanced approach. First, the EUTO Workstation Team systematically reviewed approximately 350 systems which Parks had designated as having no applications that depended on Java; the team then verified that no applications required Java on those devices (so removal would have no impact) and removed or updated the older version of Java. Next, the team used a **slow and staggered approach** to remove or update Java from all the remaining machines that were in fact running Java-dependent applications. This was a process that involved examining each instance of Java.

As of May 30, 2024, there are only **1,245 Java-related vulnerabilities left** — representing **just over 13% of the original total**. The team expects to have lowered these Java-related vulnerabilities on PCI devices to below 1,000 by mid-June.

The Workstation Team is now focused on removing or updating Java from the remaining systems, with the exception of their last hurdle in this challenge: approximately 300+ devices, some of which are kiosks that are customer or guest-facing, many fixed or built into specific locations in Disney parks and resorts worldwide, some with designated specialized printers (such as photo printers). To address the remaining vulnerabilities in these kiosks, the Workstation Team is actively testing an update process and hopes to start deploying updated Java in all kiosks by the end of Q3 — **a mere 9 months from first being assigned to take on this work**.

Close coordination and cooperation among teams, along with agility, creativity, and tenacity, have enabled the EUTO Workstation Team to achieve what at first seemed nearly impossible — all while keeping the airplane in the air.