The DATACENTER Journal
Where IT, Facilities and Design Meet

The Cost of Network Downtime

by David Bjerke and Nilson Gabela

The security and reliability of structured-cabling components in the local-area-network (LAN) and data center space is vital to the success of businesses across the globe. As the world becomes more connected, any failure that leads to downtime can cause a considerable loss of revenue and productivity, and it can lead to uncertainty among customers.

Reliable physical security, from active components to the patch panel, has proven to be elusive across the structured-cabling industry. A litany of solutions have addressed this gap; they are meant to be implemented above and beyond labeling standards. They have included smart/intelligent patching, end-point illumination and others. All of these options come with some give and take, whether it's investment in more equipment, an increase in man-hours to maintain the system, or loss of density and other features. Most solutions have an electrical end-point illumination system.

None of the available options, however, has decreased the human-error aspect of downtime. Given the low adoption rate of jumper tracking and management, as well as no decrease in human error across the industry, a jumper security and management solution continues to be elusive.

What is downtime and why does it matter?

Downtime—when a network is unable to provide its intended action or service--remains a serious threat for network managers. The consequences can wreak havoc on finances and can lead to negative perceptions of the business. The Ponemon Institute's most recent downtime study, released in January 2016, highlights a 38 percent increase in the cost of network downtime, from an average of $505,502 in 2010 to $740,357 in 2015. Estimates show downtime events continue to become more expensive as businesses and users increase their network reliance, meaning the trend will continue upward. Industries

with the highest expense include financial services, communications, health care, e-commerce and colocation. But across all industries is the absence of a physical-security solution that maintains density requirements and reduces overhead in space, material and manpower. The result is stress and uncertainty among network managers and technicians, lost revenue, and probably more lost sleep than the industry realizes.

Downtime From Human Error

Human error plays a large part in network downtime. The Information Technology Intelligence Consulting (ITIC) 2017–2018 Global Server Hardware, Server OS Reliability Report says that "survey results indicate that human error continues to be the biggest cause of unplanned reliability incidents." Ponemon's January 2016 report showed that network outages due to human error remained steady from 2013 to 2016 at 22 percent.

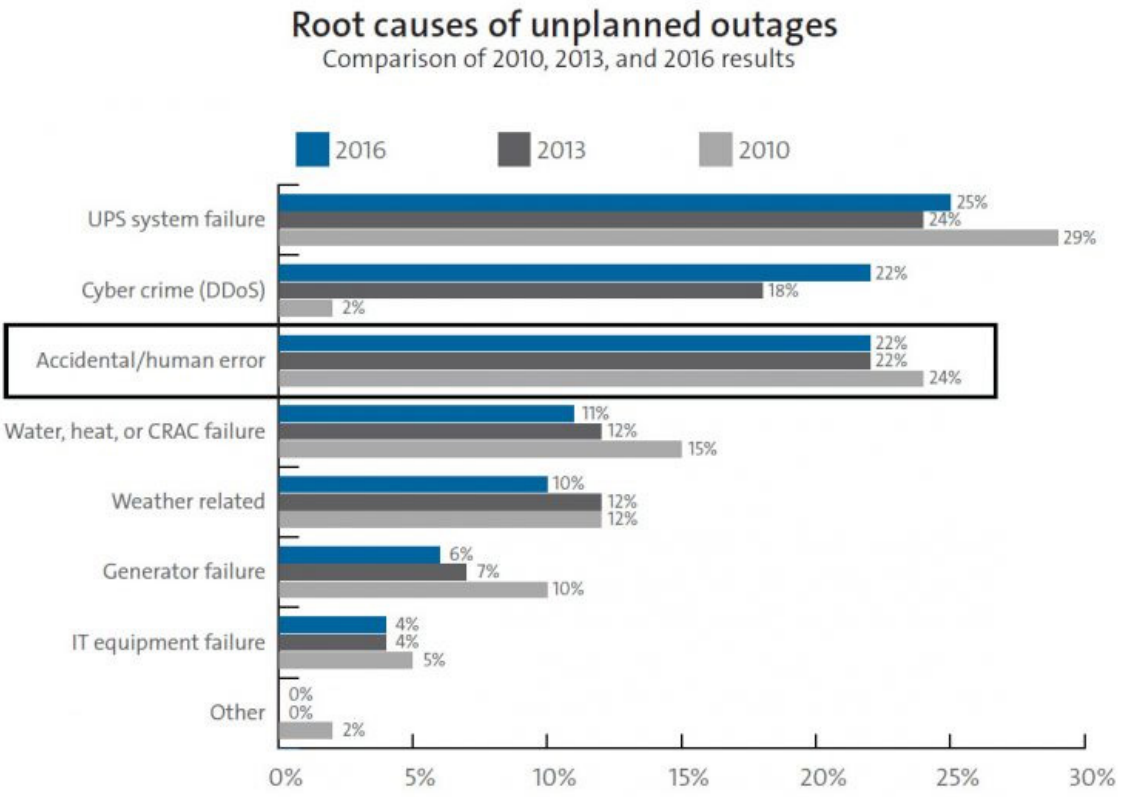
What's worse, the total cost of a human-error-related outage jumped from $380,000 in 2013 to $489,000 in 2016, an increase of over 28 percent—the largest increase of all root causes that Ponemon analyzed. This fact should send shivers down the spine of anyone responsible for moving patch cords around.

How do problems happen in this case? Jumpers and patch cords are traditionally seen as consumable items in the data center. Although many businesses have a robust labeling and safety program for jumper management, as jumper quantities increase and as moves, adds and changes (MACs) continue, initiative and hard work are necessary to ensure the labeling meets requirements. Not having a robust jumper program can lead to lax management of jumpers that are connecting expensive active components to the network. Everyone who works in a data center has a story or two about mislabeled jumpers, old labeled jumpers that were reused, unreadable labels, or numerous patches that makes finding the other end of the link difficult. How many times have you stood at a rack arguing about who was going to unplug the jumper?

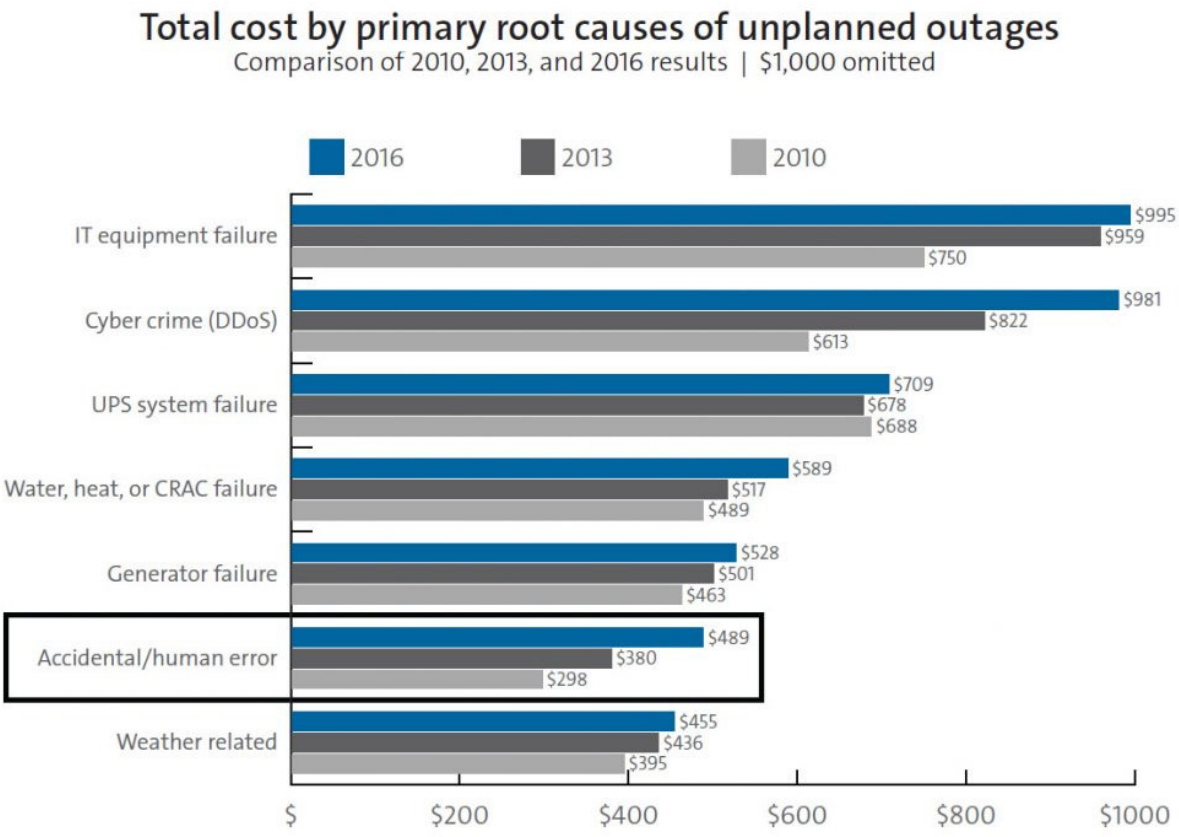
Mitigating Downtime Risk

Estimating the total cost of network downtime for businesses has proved challenging. The financial impact of an outage can typically be calculated, but the intangible aftereffects can be more difficult to quantify. These effects can include negative perceptions from customers that value and pay for a certain quality of service, continuous access and on-time results. The greater the impact that network outages have on customers, the more front-page news stories will appear on this topic.

Until the market has a viable, cost-effective solution, network managers must remain vigilant about protecting their network from unintended outages. The first step would be to estimate how much an outage costs. The company can then build a



Ponemon Institute. "Cost of Data Center Outages." Jan. 2016, https://www.ponemon.org/blog/2016-cost-of-data-center-outages.



Ponemon Institute. "Cost of Data Center Outages." Jan. 2016, https://www.ponemon.org/blog/2016-cost-of-data-center-outages.

business and then balance investment in network security with the risk and cost associated with an outage. Second, technicians on the front lines must maintain strict accountability of network assets, to include the management of jumpers. A robust program should adhere to current labeling standards and meet the company's needs. In addition, the company should implement a safety program that ensures all personnel who physically touch the network, including new hires, are trained to know business rules, labeling schemes, layout and procedures for MAC work.

Conclusion

The needle hasn't moved in a positive direction with regard to human error, network downtime and viable, cost-effective physical-network solutions. Although eliminating human error and material failure from the network is impossible, there must be a more concerted effort to ensure that physical-network security reduces the human-error aspect of network downtime. Until then, CEOs down to network managers and technicians will continue losing sleep over the prospects of an outage that could be prevented by implementing a physical-security program. When a solution to patch-cord and jumper security arrives—one that increases reliability and security without compromising manpower and density requirements—the market will be willing to adopt it, as long as it decreases the human-error aspect of network outages.

About the Authors: David Bjerke, senior product specialist for cable assemblies, has been with Corning for four years. Before this role, David was an enterprise-networks sales engineer in Iowa and Nebraska. David has a degree in computer science.

Nilson Gabela, global-market development manager for data centers, has been with Corning for 15 years and spent time in the Engineering Services and Sales groups. In these positions, Nilson has navigated his way in and out of international data centers both large and small. He has a degree in mechanical engineering and an MBA.

This article was originally published on August 31, 2018 on www.datacenterjournal.com