# PROPERTY

COMMENTARY PAPER

## Kim Kardashian's private equity firm, social media influencers and property claims

COMMENTARY PAPER

# Kim Kardashian's private equity firm, social media influencers and property claims

## Social media content

On September 7, 2022, news broke that Kim Kardashian's newest business venture is a private equity (PE) firm. PE firms invest in start-up companies and mature businesses with the goal of increasing their value before selling them. Some of our favorite brands are backed by PE firms. From Airbnb to PetSmart, Panera Bread, Uber and Spotify, PE-funded companies are all around us. The funds deployed to acquire these companies are raised from pension funds, endowments and wealthy individuals, among others.

Kim is known as a "mega-influencer" for being a highly visible person on social media and generating a great deal of user engagement, specifically on Instagram among her 330 million followers. This means that when Kim posts about consumer products, those products can become best sellers virtually overnight. David Friedberg, an early Google executive and one of the "besties" on the All-In podcast, recently explained that due to the power of democratized media, private YouTube channels or podcasts for instance, there are now thousands of individuals that have solidified themselves as a brand. This was achieved as a result of content they published and continue to publish daily on platforms such as Instagram, YouTube, Twitter and others. This means that when Kim will invest in a company via her PE firm and promote that company through her various social media platforms, a great deal of interest in (and likely sales of) their products will surely follow.

So, how does this relate to property claims? Influencers all have in common their use of social media platforms being housed on computer servers. While many of the larger platforms operate their own data centers (Google/YouTube, Meta/Facebook and Instagram), others pay for data center operators, such as Amazon Cloud Services and Microsoft's Azure Cloud Computing, to house their applications. This means that when something unfavorable happens in the data center, business income (BI) losses can mount quickly.

## Data centers

Data centers are secure, temperature-controlled structures that incorporate large backup power generators. Companies utilize data centers to house critical applications and data. Equipment racks are populated with network routers and switches, uninterruptible power supplies (UPS), internet security firewalls, hard drive storage systems, data processing computer servers, and various controller modules for application delivery.

Today, data is stored and connected across multiple data centers, the edge, as well as public and private clouds. The edge data centers are smaller structures that are located at the edge of the network infrastructure. As such, edge data centers are closer to users and devices.

## Common causes of damage and equipment vulnerabilities

While data centers are theoretically designed to withstand harsh environmental conditions such as hurricanes, tornadoes or earthquakes, they are still susceptible to damage that would trigger a property claim.

**Improper installation**

A data center in Sweden experienced a fire caused by an arc flash in an overhead electrical busway, an enclosure that houses copper bars that conduct electricity. The busway – assembled in 10 feet long sections – distributes power within the data center. Investigators determined that the bolts secured by two busway joints were not tightened (torqued) properly when initially assembled. Over time, the loose connection caused a thermal avalanche, causing the joint to fail.

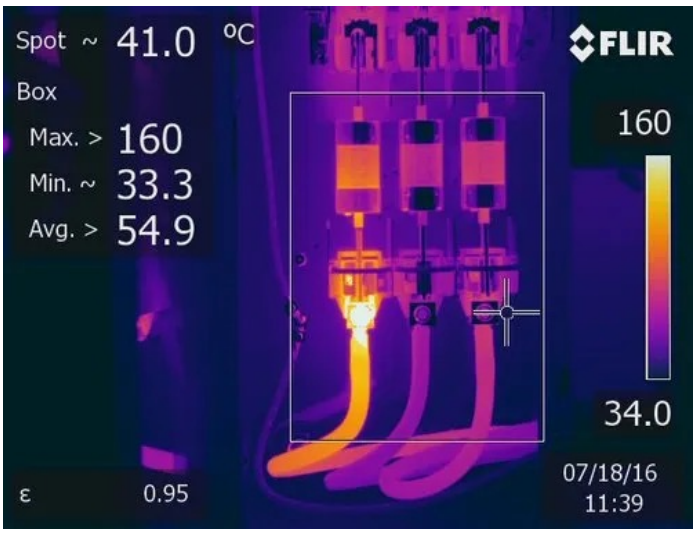
**Facility maintenance**

A data center in New Mexico experienced water exposure. Roofers were scheduled to perform extensive roof repairs, although all parties overlooked the forecasted weather. Rainwater exposed a portion of the racked equipment.

**Equipment failure**

A data center experienced smoke exposure because of a fire in an adjacent building. The cause of the fire was a failed UPS battery. The UPS was connected to the data center through an underground conduit, which is how smoke and soot penetrated the building.

Another example includes a brand-new power distribution unit (PDU) in a North American data center. A PDU is a sizeable cabinet that distributes electricity from the building's primary power to multiple devices within the data center. In this case, the PDU was suspected of starting a fire as a result of a glowing connection.




The National Fire Protection Association (NFPA) describes a glowing connection as follows: "When a circuit has a poor connection such as a loose screw at a terminal, increased resistance causes increased heating at the contact, which promotes the formation of an oxide interface. The oxide conducts current and keeps the circuit functional, but the resistance of the oxide at that point is significantly greater than in the metals. A spot of heating develops at that oxide interface which then becomes hot enough to glow. If combustible materials are close enough to the hot spot, they can be ignited". In this instance, a forensic analysis of the PDU revealed that two electrical busbars were connected with a bolt, although the bolt was not tightened properly.

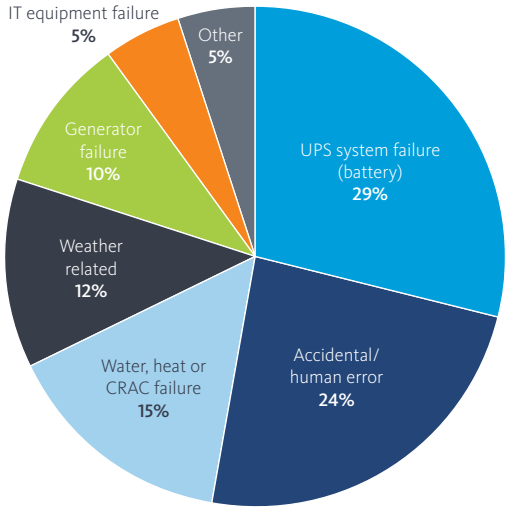
**Insufficient or misconfigured backup power**

Power failures are a common reason data centers experience business interruption. As a result, data centers incorporate redundant power in case their primary power is interrupted. Batteries and/or generators are the common backup. If batteries are not maintained properly or replaced as scheduled, generators are not tested, and power failure tests are not conducted on a regular basis, redundancy power will likely not be available when it is needed most.

**Cooling failures**

Data centers generate a great deal of heat. Cooling equipment continuously is required to prevent overheating. Heating, ventilation and air conditioning (HVAC) systems can stop working as a result of misconfigured controls, lack of preventive maintenance, power surges, and lightning. Examples are illustrative, not exhaustive. It is important to note that HVAC systems do not need to fail to cause the computer equipment to overheat. The equipment may overheat because of an inadequate cooling infrastructure, which causes hot spots within high density racks.

**Primary root causes of unplanned data center outages**



Some computer manufacturers design server equipment with the ability to continuously log internal temperatures. The server can power itself off, as a self-preservation measure, if the ambient temperature exceeds the specified working threshold. Unfortunately, this is not a uniform practice across all manufacturers.

**Wet pipe sprinkler fire suppression**

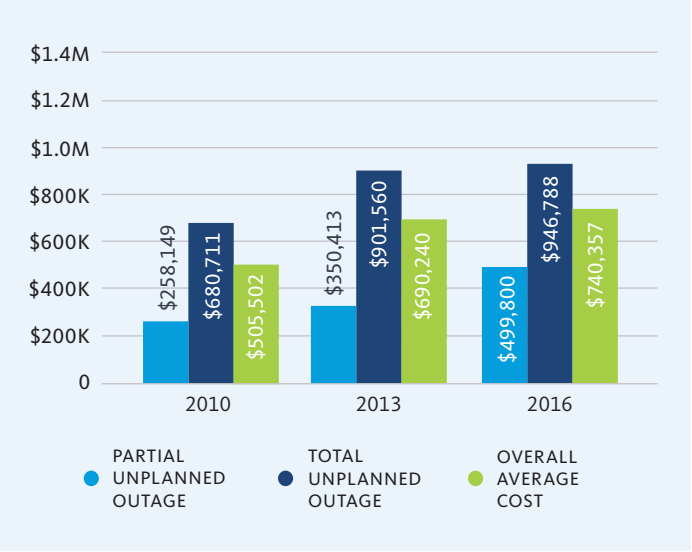
A wet pipe sprinkler system is always water-filled and is therefore not a preferred suppression solution in data centers. Most modern data centers use non-water fire-suppression solutions, so they do not damage equipment if purposefully or accidently triggered. Many older data centers still incorporate wet suppression systems. Water leaks and accidental discharges have caused major outages.

**Cyberattacks**

Within data centers, power systems, computer servers, storage units and network functionality gear are all vulnerable to cyberattacks.

## Quantifying the cost of data center downtime

Ponemon Institute published a study (commissioned by Vertiv) titled, "Understanding the cost of data center downtime". The study analyzed enterprises with revenue models that depend heavily on a data centers' ability to deliver information technology (IT) and networking services, such as e-commerce companies. For such companies, network downtime can be particularly costly. The study, concluded in 2011, is dated, although at the time network downtime translated to lost revenue of between $593 per minute to more than $11,000. In a 2016 revision, those figures increased to $926 on the low end to over $17,000.




The bar chart on the left compares the costs of partial unplanned outages and complete unplanned outages, per occurrence. It is important to note that the longest partial unplanned outage was recorded at 134 minutes and the total unplanned outage was 119 minutes. Commercial adjusters are cognizant that tornado, fire and water loss recovery times are not measured in minutes. Restoring equipment can take days, weeks and even months. Based on the 2016 study revision, one day would equate to business interruption losses between $1.3M - $24.4M. For comparison purposes, Amazon's 2021 revenue was $469.8bn. That translates to $893K per minute or $1.28bn per day. Expedia, the popular online travel agency, recorded 2021 revenue of $8.6bn. This figure equates to $16.3K per minute and $23.5M per day. The data shows that the study analyzed small and sizable businesses.

The Westside Story published an article about a Samsung data center that sustained fire damage. According to Jayaram Pawar, "A fire at Samsung's backup data center in Gwacheon, South Korea, knocked off service to television Smart Hub menus, smartphones and every other gadget that utilizes the servers in this particular data center. Service was out for a few hours before being restored. The Samsung App store and any apps that needed communication with the servers for a particular operation, were rendered inoperable during this outage, along with any 3rd party applications that required server authentication before launching."

Pawar goes on to say that "This was yet another incident which involved fire as there was one back in March at Samsung's partner facility that manufactures printed circuit boards (PCBs) for Samsung Galaxy S5, which came as a setback for the Android giant in mass production of the phone just before the launch. Though we do not know the extent of loss for its datacenter accident, the PCB fire incurred a loss of $1 billion, and took 264 firefighters, 81 vehicles and 8 hours to contain."

## Commercial property claims

Adverse weather, improper installation, facility maintenance, equipment failure, insufficient or misconfigured backup power, cooling failures, wet sprinkler fire suppression discharges and cyberattacks all impact data centers on a regular basis. Considering that a great deal of marketing dollars are now spent on social media content as the primary driver of consumer product and service growth, every minute that a platform cannot function as intended results in costlier BI. Retaining experts that are fully versed in data center damage mitigation and functionality restoration is critical to managing the project scope and the carrier's overall exposure.

## About EFI Global

EFI Global, part of Sedgwick, is a well-established brand with an excellent reputation in the Americas, Africa, Asia-Pacific and Europe as a market leader in environmental consulting, engineering failure analysis and origin-and-cause investigations. Each year, EFI Global completes more than 45,000 projects worldwide for a wide range of clients, such as commercial, industrial, institutional, insurance, government, risk managers, public and private entities. EFI Global is one of the world's most respected emergency response firms, capable of providing practical solutions to the most complex problems. Our multidisciplinary team of first responders, project managers, engineers, geologists and scientists are selected for their technical proficiency and in-depth industry knowledge to aid clients in resolving technical problems. For more, see **efiglobal.com**.

## Resources and references


- Ponemon Institute research report sponsored by Vertiv. Cost of Data Center Outages, Data Center Performance Benchmark Series. January 2016
- Ponemon Institute research report sponsored by Vertiv. Calculating the Cost of Data Center Outages. February 2011
- Vertiv. Understanding the Cost of Data Center Downtime, An Analysis of the Financial Impact on Infrastructure Vulnerability. 2016


## Get in touch with an expert


**David Beachy, MS, PE, CFEI, Service line principal, principal engineer**

David Beachy is a licensed professional engineer in multiple states throughout the mid-Atlantic region. Mr. Beachy has more than 13 years of engineering experience and six years focusing on conducting loss investigations and providing consulting services on the topics of civil, mechanical, and fire protection engineering. For more information, contact **David.Beachy@efiglobal.com**.



*caring counts* | efiglobal.com