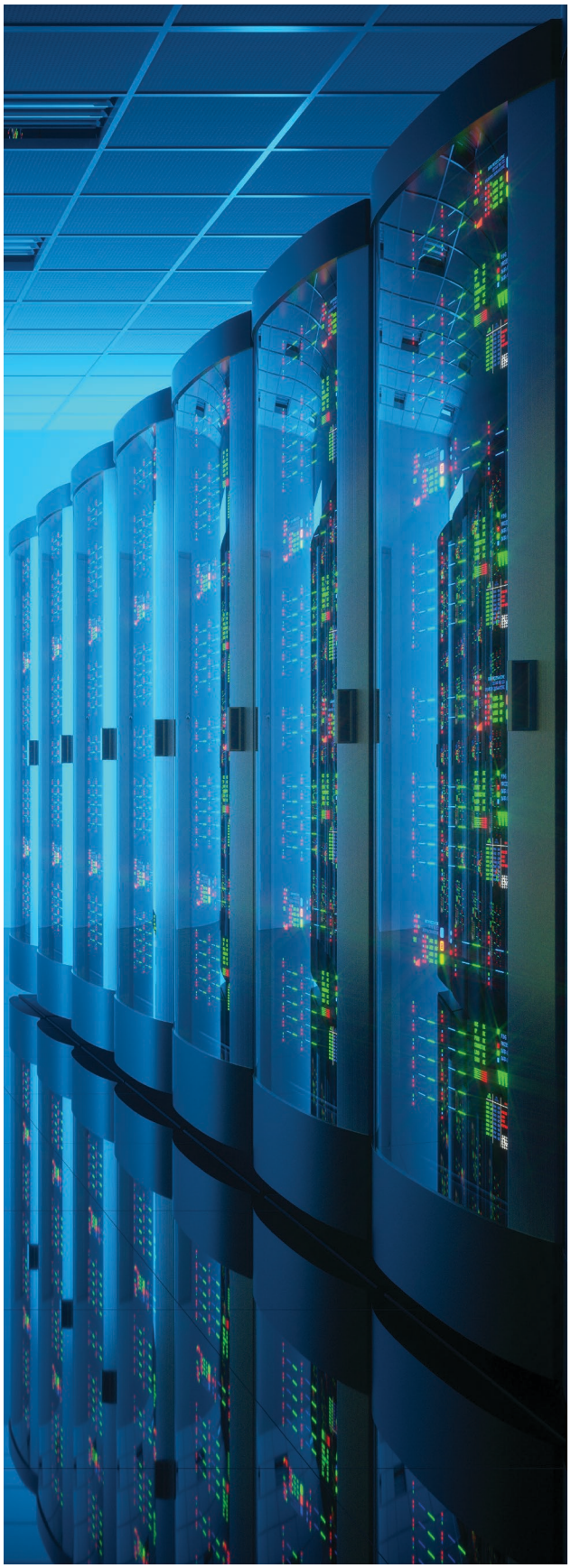
INSIGHTS | MARCH 2020

Digital Deception: Is Your Business Ready for "Deepfakes"?

ABC Shoe Corporation has just completed the most successful quarter in its history. The CEO holds a press conference to announce the good news. Several hours later, an altered video of the CEO at the press conference goes viral on social media, showing him slurring his words and appearing inebriated. ABC Shoe Corporation has become a victim of a "deepfake."

This story may seem farfetched, but similar incidents have already played out in real life, impacting mostly politicians and celebrities. Businesses too are starting to see deepfakes targeting them. What once took significant skill and time to create can now be done cheaply, quickly, and convincingly, posing a major threat to both public and private sectors.

A "deepfake" is a sophisticated digital forgery of an image, sound, or video. The forgery may be so good that a human is unlikely to detect the manipulation. The goal is to mislead and deceive, making it appear as though a person has said or done something when that is not the case. Supported by advances in artificial intelligence, deepfakes have proliferated across the internet as the technology becomes less expensive and more accessible.



Risks for Businesses

Businesses have always taken great strides to protect the "CIA" triad of information security — confidentiality, integrity, and availability. Data confidentiality has frequently been threatened by massive data breaches involving businesses, while attacks on the availability of data have become a new normal with the proliferation of ransomware attacks.

Attacks on data integrity, however, appear to be a more recent phenomenon. And businesses may not be prepared to respond to this sleeping giant, one that could have devastating impacts.

Nation-states, competing businesses, disgruntled employees, criminals, and anonymous saboteurs may use deepfake technology to disrupt business operations or facilitate fraud. Indeed, news reports surfaced in August 2019 that — for the first time — deepfake audio technology was used to mimic the voice of a CEO to facilitate the fraudulent transfer of funds. This type of misuse introduces a potentially dangerous trend.

Deepfakes can also have a severe impact on a company's reputation. A deepfake posted on social media could easily go viral and spread worldwide within minutes. Companies would have to spend valuable resources identifying, removing, and rebutting such fake content; legal fees and crisis management expenses would likely also stack up. If the deepfake was embedded in internal materials, companies would need to investigate the network intrusion and remediate corrupted systems and data. Though a company might ultimately prove it was the victim of a deepfake, the damage to its reputation will already have been done, potentially resulting in lost revenues.

Current Legal Regime

As with many advances in technology, deepfakes are outpacing the law. While no law directly addresses deepfakes, several criminal and civil laws may be applicable.

Criminal statutes governing fraud, extortion, and cyberstalking, for example, may broadly serve as criminal remedies and deterrents to combat deepfakes. Federal securities law may also apply to a deepfake used to defraud anyone in connection with registered securities. Impersonating a government official through a deepfake could also result in criminal penalties.

Civil remedies provide more flexibility for businesses in holding deepfake perpetrators accountable. Unlike criminal remedies, if a business can prove a general harm, such as defamation, copyright infringement, or a violation of the right of publicity, the business can sue the perpetrator.

Knowing exactly whom to bring actions against and being able to bring perpetrators under the jurisdiction of US laws — particularly if they live abroad — may be difficult. If a deepfake is spread over the internet, however, the victim business will likely only be able to sue the perpetrator of the deepfake. Content platforms, even when hosting fake content, are typically immune from civil liability under US law.

Protecting Data Integrity

Risk managers can take action now to build enterprise resilience and address the potential onslaught of new data integrity threats. Public relations and crisis communication planning — along with identifying properly legal remedies — can be critical to responding to a deepfake and mitigating reputational harm. Cyber risk assessments and strong cyber hygiene can also help thwart attacks that are targeting data on company networks, while robust backup procedures can help restore or verify corrupted information.

For those businesses that fall victim to a deepfake, cyber insurance policies may provide relief for some financial loss.

A data integrity attack on a company network, like other cyber-attacks, could result in a security incident that would need to be investigated and remediated. Cyber insurance policies often offer broad cyber event management coverage for the cost of crisis communications and computer forensic specialists responding to an incident. If data has been corrupted, cyber insurance policies may cover the cost to replace, restore, or recreate the data. A cyber policy may also respond to a ransom demand linked to a deepfake on a corporate network.

Cyber policies are also expanding to include coverage for attacks on a company's reputation from adverse publicity after a cyber incident or privacy breach. For example, a cyber policy can cover lost revenues and the costs to hire public relations consultants after a reputational attack. While wordings vary and are often tied to a network intrusion, these coverages continue to evolve and could be helpful to a company that suffers reputational harm from a damaging deepfake.

Crime policies — and, to a lesser extent, cyber policies — could also help companies that have fallen victim to deepfakes recover funds that were transferred to third parties under false pretenses.

Deepfakes are a new type of threat for businesses, and insurers are still assessing potential risks. Whether a cyber policy responds to a deepfake ultimately depends upon the circumstances of the incident and the terms and conditions of the policy. Risk managers should carefully review their policies and work with their insurance advisors and legal counsel to assess potential exposures and coverages for this evolving threat.

This article was previously published by Business Insurance.

For further information about deepfakes and other cyber risk topics, please contact:

STEPHEN VIÑA
Senior Vice President, Marsh
+1 202 263 7919
stephen.vina@marsh.com
cyber.risk@marsh.com
www.marsh.com

STEVE BUNNELL
Former General Counsel,
Department of Homeland Security