Q How relevant is the threat posed by deep fakes, and how should that threat be evaluated?

A "Deep fake" is a term derived from deep learning, and it refers to modifying or creating fake videos using human image synthesis and artificial intelligence (AI). Although it started as academic research, it has the potential to create hoaxes and personal attacks by creating fake pornography and fake news by using politicians' faces to create fake videos. Digital fakery is not new, but it has morphed from photos to edited videos. Face swapping techniques are not new either. But now, with deep learning by machines, these tricks can be automated, and the tools are accessible to many more people. The big problem is that current forensic tools are not able to detect this fakery.

Fake news, also known as junk news or pseudo-news, is a type of yellow journalism or propaganda that consists of deliberate disinformation or hoaxes spread via traditional news media (print and broadcast) or social media. Frequently, fake news uses deep fake videos and spreads through social media. Although most social media sites have policies to ban deep fake pornography, other videos are not explicitly banned. The main challenge is that applications for generating deep fakes are available on the Internet, and anyone with malicious intent can target a person or organization by creating fake videos and fake news. As the technology is being developed, identifying fake videos is becoming more and more difficult. Deep fakes are now used in the world of cybercrime. Fraudsters successfully used deep fake video to cheat the chief executive officer (CEO) of an energy company out of US$243,000.[1] The victim transferred the funds into the account of the fraudsters because he believed the impostor who had impersonated the executive's parent company CEO's voice pattern and accent. The demand was made with the pretext of paying a supplier, and a promise was made that the funds would be reimbursed. After the victim made the payment, the money was transferred from Hungary to Mexico. Suspicion arose when the fraudsters called the victim again to demand another payment. The insurer of the victim has issued reimbursement for the loss incurred.

Deep fakes and other AI-based technologies are being used more frequently in the fields of cyberfraud and fake news. What we see and hear can no longer be assured to be a true representation of the source of the information. Until recently, biometric-based security systems were considered to be state of the art. However, in the current age, when most technologies are accessible in the open-source space, hackers are resorting to unique methods. They are actually hacking biological information, fingerprints, faces, voices and effectively combining them to either misrepresent or steal information and money.

Q Our organization's first cybersecurity audit is due shortly. What guidance can we enlist to prepare to coordinate the audit?

A Information systems audit is a process for determining the extent to which policy, procedure, standards and practice combine to provide a safe and secure environment to the users and other stakeholders. The IS audit process, therefore, must contain a detailed evaluation of all the high-risk scenarios that the organization has evaluated and seek to determine if every control that is put in place to either mitigate, transfer or accept the risk will provide the outcome the organization

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sw1FVV

desires. Considering this objective, organizations must welcome the audit as an opportunity for improvement rather than a necessary evil.

First and foremost, the organization's leadership should own the audit and ensure that it is given due importance in terms of allocating resources and reviewing the progress made on a regular basis. One way of ensuring such support is to identify a single point of contact at the organizational level and at each auditee area level. This helps when planning the auditor's meetings, visits and testing of controls in each auditee area. Once there is full awareness of the fact that auditors review risk assessment results and then prioritize the controls to be tested, the same method can be adopted to determine the auditor's visits.

Information systems auditors focus on reviews of security controls. These reviews cover three aspects:

1. Design of controls based on the risk they mitigate
2. Implementation of controls if they have been implemented as per design and mitigate the identified risk
3. Effectiveness of control, which focuses on ensuring that a control is effective all the time. Once an effective control is established, the auditor concludes the assessment of the effectiveness of the controls implemented.

To arrive at a conclusion, the auditor needs to review the control design, which is generally based on risk assessment results. Design of controls typically involves a review of security policies, baseline configuration for IT infrastructure and documentation of activities that will help ensure that the controls live up to their objectives. Hence, a risk register and risk profiles are initial records for which auditors are looking. Additionally, auditors need evidence of support by senior management for information security initiatives. To that end, auditors interview the members of senior management and also check for exceptions granted to members of senior management.

Based on the risk assessment results, the auditor then verifies the design of controls. For this, auditors typically use some global standard (e.g., International Organization for Standardization [ISO] ISO 27002 or the US National Institute of Standards and Technology [NIST] Special Publication [SP] SP-800) to benchmark the organization's security program. Use of standards ensures that auditors are not missing any area of security.

Design of control refers to the activities associated with controls. For example, how does the change management process work? First, an auditor reviews process documents and tries to determine if the processes meet all the requirements of risk mitigation. Then, the auditor interviews users to corroborate that the processes are executed as documented. This is design phase checking. The evidence needed for this phase includes process documents and interview notes.

"TO ARRIVE AT A CONCLUSION, THE AUDITOR NEEDS TO REVIEW THE CONTROL DESIGN, WHICH IS GENERALLY BASED ON RISK ASSESSMENT RESULTS."

In control implementation testing, the auditor reviews the implementation of controls. In the example used herein, the auditor asks for the list of changes that took place during the period of audit. The list is reviewed and then the auditor selects one change that requires all activities of the change control process to be executed and verifies the record for each activity (i.e., request for change, assessment of impact due to change including need for change, risk associated with change, risk mitigation plan for change, urgency of change, approval of change, execution of change, acceptance testing of change, notification to all stake holders about implementing change, implementing change with fall back arrangements) in case problems arise after the change implementation. This covers the implementation review.

The last phase of the audit is control testing (i.e., checking effectiveness of controls). The auditor reviews more samples from the list of changes that occurred in the time span covered by the audit to ensure that the process is followed uniformly.

The auditor follows a similar process for all controls. For control activities that are automated, the auditor may not select samples for review but ensures that the organization has control over the configuration of controls. For example, implementing password policy (i.e., complexity, length, duration of password, period for changing the password) can be configured within a system. The auditor reviews the configuration to determine whether it is in line with password policy. Then, the auditor verifies who can change this configuration and also reviews activity logs for the users who have access to changing the configuration to determine when it was last updated. This helps the auditor confirm that password policies are implemented properly. In this case, the auditor may ask for screenshots or printouts of configuration and activity logs.

Before closing the audit, the auditor may discuss the findings with auditee management. It is preferable that all levels of management attend this meeting so that findings can be understood with better perspective. If the auditor is an external independent auditor, it is likely that the auditor's knowledge about the organization's processes may not be as clear as management's and the findings may not be most relevant. Attending this meeting ensures that the auditor and management share similar understandings. Sometimes, the auditor may need to retest some controls. In some cases, management may not agree with the findings of the audit, and these issues can be resolved in this meeting.

Generally, records to be presented to the auditor can be ascertained from the control process documentation.

Implementing control self-assessments also helps in understanding the auditor's objectives, and auditees can be ready with records and evidence the auditor might require. This helps reduce the audit time.

Endnotes

1 O'Donnell, L.; "CEO 'Deep Fake' Swindles Company Out of $243K," Threatpost, 4 September 2019, *https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of-243k/147982/*

Answers: Crossword by Myles Mellor
See page 54 for the puzzle.