الغزاوي ومشاركوه
AlGhazzawi & Partners

MITIGATING CYBERSECURITY RISKS IN THE POST-PANDEMIC REMOTE WORK ERA

The transition to remote work models in the post-pandemic era has significantly increased exposure to cybersecurity threats and data privacy breaches, compelling enterprises to adopt measures to mitigate such risks. Mobile working involves accessing work networks from external channels, expanding the range of cyber-attacks, data leakage, data storage, and system operations outside corporate infrastructure. Subsequently, data breaches and infringements can result in severe legal and commercial consequences. This report aims to identify the common cyber threats commercial enterprises encounter and propose systematic solutions to mitigate these risks.

Potential Threats to Security

Data Breaches

Data breaches occur when secure, confidential, or protected information is accessed, disclosed, or stolen without authorization.[1] This can happen through various means such as hacking, insider leaking, or the loss of physical devices containing data.

The risk of such acts was exposed in 2007 when HSBC bank lost an unencrypted CD containing sensitive data of 370,000 customers, which was sent via regular postal mail but never arrived.[2]

This resulted in a significant breach of trust, as personal and financial information was exposed.[3] The Financial Services Authority (FSA) fined HSBC £3 million in 2009 for inadequate data protection.[4] The incident caused substantial reputational damage and impacted HSBC's relationships with customers and stakeholders.[5]

The commercial viability of cybercrime has expanded the market, as it has become increasingly easier to purchase and rent tools and services for hacking purposes. User credentials are valuable to hackers because they allow continuous unauthorized access to various online accounts, posing a risk to virtually anyone with an online presence.

In early December 2022, PayPal experienced a credential stuffing attack affecting about 35,000 accounts.[6] The attackers used credentials obtained from other data breaches to access these accounts.[7] Although some sensitive information was potentially accessed, including Social Security numbers and addresses, no unauthorized transactions were detected.[8] PayPal responded by resetting affected passwords and offering free identity monitoring services.[8]

The dangerous possibilities of the virtual theft of consumers' personal information were rendered evident in 2014 when Yahoo was the target of a significant cyber-attack where hackers, allegedly state-sponsored, accessed and stole data from 500 million user accounts.[9]

The stolen information included names, email addresses, phone numbers, birth dates, and encrypted passwords.[10] Yahoo publicly disclosed the breach in 2016, marking it as one of the largest known data breaches in history.[11]

This incident raised major concerns about cybersecurity practices and the protection of personal information online. A third type of data breach involves cyber threat actors who target large companies for cyber intrusions to spy, steal data to sell, and extort money from victims. In 2016, hackers stole $101 million from Bangladesh Bank after infiltrating its computer systems for nearly two weeks.[12]

They used malware to manipulate the bank's servers, making the transactions appear legitimate and deleting logs to cover their tracks.[13]

The sophisticated operation, potentially conducted by a financially motivated criminal group, involved transferring money to accounts in the Philippines and Sri Lanka.[14] The heist highlighted vulnerabilities in the bank's systems and led to significant repercussions, including the resignation of Bangladesh Bank's governor.[14]

These four diverse instances evidence the distinct forms of data breach terrorizing today's virtual world, posing significant security threats to both the individual and the global enterprise.

هيئة الخدمات المالية
FINANCIAL SERVICES AUTHORITY

AlGhazzawi & Partners

Understanding Data Breaches [1]
HSBC's 2007 Data Loss Incident [2,3,4,5]
PayPal's 2022 Credential Stuffing Attack [6,7,8]
Yahoo's 2014 Cyber-Attack [9,10,11]
The 2016 Bangladesh Bank Breach [12,13,14]

Artificial Intelligence &Data Manipulation

Yet, in a fast-evolving digital world, traditional hacking techniques have long been eclipsed by advanced tools like AI technologies and Machine Learning algorithms.

AI-driven technologies can perform complex tasks such as interacting with users in a convincingly human-like manner, which can be exploited for social engineering attacks where individuals are tricked into revealing sensitive information.[15]

The artificial intelligence research organization, Open AI, recently exemplified these dangers, when the enterprise informed users that it could not delete specific prompts from users' history, and thus advised against sharing sensitive information on the platform.[16]

Moreover, there are significant menaces involved in the ability of machine learning algorithms to process large datasets, and identify patterns and system vulnerabilities, because malicious actors can manipulate AI models to generate false, deceptive output.

One such case occurred in February 2024, when a Hong Kong-based multinational company lost $25.6 million in a deepfake scam.[17]Scammers used AI technology to create realistic video imitations of the company's CFO and other staff members during a video call, convincing an employee to transfer funds.[18]

Despite initial doubts, the employee was persuaded by the convincing deepfakes and made 15 transfers before realizing the scam a week later.[19] Hong Kong police have arrested six people in connection with the incident.[20]

This incident highlights how novel technologies, such as hyper-realistic "deepfake" AI videos, make it increasingly difficult to distinguish between real and fake output.

Exposing the risks of implementing AI in the processing of confidential information, these examples evidence the devastating consequences of potential data breaches, targeted or accidental, facilitated through novel technologies.

PHISHING

Phishing is a specific type of cyber-attack that fools individuals into revealing personal information, such as passwords or credit card numbers, through deceptive communications.

Phishing can also be conducted via text messages or social media, although it is most commonly associated with email-based attacks.

These emails often appear to be from reputable sources, such as major banks or trusted companies and may include links to fake websites that closely mimic legitimate ones.

Opening this malicious link may result in malware infecting the individual's computer and provide a foothold into the system through which the hackers can further exploit sensitive information.

Pretexting differs from phishing as it often constitutes a more personalized, direct attack on the individual.

This back-and-forth communication builds trust and makes the target more likely to fall for the scam.

AlGhazzawi & Partners

AI and Machine Learning [15]
OpenAI's Warning [16]
Deepfake Deception [17,18,19,20]

Cybersecurity & Data Protection

Regulatory Landscape in Saudi Arabia

Anti-Cyber Crime Law of 2007 serves as a foundational legal framework in the Kingdom of Saudi Arabia. This law applies to all individuals and organizations, including companies and government entities. This means that no one is exempt from following the regulations set by this law.

The law classifies crimes defined in the said law, and the laws enacted following the precedent law [referred below] provide general guidelines for data protection (i.e., data integrity, confidentiality, and deterrent effect). The law criminalizes possession, creation, and distribution, of data and other forms of computer misuse tools and cybercrimes that threaten the integrity of digital information.

In addition to the Anti-Cyber Crime Law, other laws and regulations also influence the provision of communication services and the operation of networks. The primary law governing the processing of personal data in the Kingdom of Saudi Arabia is the Personal Data Protection Law (PDPL).

The law confers rights to individuals which include, inter alia, the right to be informed about the processing of their personal data, the right to access such data, and the right to request the rectification or erasure of their personal data. Regulations covering the Transfer of Personal Data Outside the Kingdom are issued according to PDPL, which sets out restrictions on data transfer outside Saudi Arabia.

Several sector-specific regulations have been issued to further strengthen the cybersecurity landscape across various sectors. The Telecommunication and Information Technology Act (TTITA) governs data protection and cybersecurity across the businesses engaged in providing telecommunications and information technology services, including those offering digital content platforms, telecommunications infrastructure, and IT-related devices.

It also applies to companies that build and operate their own internal, private telecommunications systems. In case of non-compliance with the Act, the penalties can include fines, suspension or cancellation of licenses.

For the burgeoning field of the Internet of Things (IoT), the IoT Regulatory Framework is issued according to TTITA which provides detailed guidelines for the secure and efficient deployment of IoT technologies in the Kingdom. The framework sets out rules to ensure that data collected, stored, and transmitted by IoT devices is secure and that these devices are protected against potential cybersecurity threats.

The Cloud Computing Services Provisioning Regulations establish a regulatory framework governing cloud services offered to cloud customers with a physical address in Saudi Arabia. This framework applies to any service provider that owns, operates, or manages data centers or offers elements of cloud services, located within or outside the Kingdom.

All organizations affiliated with the Saudi Central Bank must comply with the 2017 Cybersecurity Framework, which regulates cybersecurity in the financial sector. This framework applies to banks, insurance and reinsurance companies, financing companies, and credit bureaus regulated by the Saudi Central Bank.

OTHER REGULATIONS ADDRESS DATA PRIVACY & SECURITY ACROSS MULTIPLE SECTORS

For instance, the Law of Practicing Healthcare Professions requires healthcare professionals to keep patient information confidential.[21] The Implementing Regulations of the Income Tax Law mandates that taxpayers are required to keep their records in the Kingdom.[22]

The Labour Law stresses that certain records must be retained at the workplace.[23] Additionally, the Banking Control Law prohibits the disclosure or misuse of confidential information obtained during banking activities.[24] Finally, the E-Commerce Law governs data privacy and cybersecurity in electronic commerce, requiring businesses to implement measures to protect personal data and secure transactions.[25]

AlGhazzawi & Partners

[21]Article 21
[22]Article 55
[23]Article 17
[24]Article 19
[25]Article 5

RECOMMENDATIONS

The PwC report highlights a critical issue that companies in the Middle East tend to focus heavily on investing in cybersecurity technology, often at the expense of other essential components of a robust cybersecurity strategy.[26]

This approach can lead to a false sense of security, where organizations believe that simply having advanced technological tools in place will protect them from cyber threats.[27]

However, it's a multi-dimensional issue that requires a balanced integration of technology, people, processes, and governance for success.[28]

To prevent and protect against these multiple forms of attack, enterprises can strengthen their business processes against cyber threats by considering the following proposed solutions, either in part or in full, as examples of effective measures

AI POLICY

In order to prevent the inappropriate input of sensitive client data into AI systems, it is essential to establish a comprehensive company policy on AI usage.

This ensures the protection of confidential information and compliance with Personal Data Protection laws.

Employers incorporating AI should develop and regularly update policies governing generative AI use and enforce these policies diligently.

The AI use policy should streamline the following: specifying which employees may use AI and the requirements for prior company approval, determining permissible tasks, and making employees accountable for outcomes.

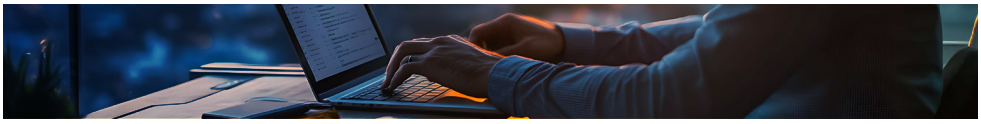
The policy should also prohibit the submission of trade secrets and other confidential information, mandate usage logs and reporting, and provide training on permissible AI use.

By doing so, companies can safeguard sensitive data, maintain compliance with evolving legal standards, and ensure responsible AI implementation in the workplace.

AlGhazzawi & Partners

PwC report[26,27,28]

Remote Working Guidelines



Companies must consider implementing the Remote Working Guidelines, specifically the Telework Cybersecurity Controls (TCC) policy proposed by the National Cybersecurity Authority in the Kingdom of Saudi Arabia. The TCC policy aims to ensure that remote work is conducted securely.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

These controls include secure VPN access, endpoint protection, and secure file sharing. It provides straightforward technical steps to enhance security in remote work environments, ensuring that sensitive data and communications are protected.

Training &Awareness

Another crucial step is to educate staff and clients on best practices for recognizing IT risks and vulnerabilities. This empowers them to identify potential security threats while working online or using computer systems.

Equipping individuals to become independently data-savvy, education enables the correct identification of security threats that may occur when working on online virtual systems.
This can include training sessions, informational materials, and regular updates on emerging threats and how to protect sensitive information effectively.

AlGhazzawi & Partners

Written by
Majid Al Harbi
Trainee Lawyer
AlGhazzawi & Partners

Reviewed by
Talal Faisal Alfi
Senior Associate
AlGhazzawi & Partners