ADGM Academy Research Centre

Article SERIES

CYBERSECURITY THREATS IN THE UAE FINANCIAL SECTOR: EXPERT INSIGHTS AND EMERGING CHALLENGES

In today’s digital economy, the UAE financial sector plays a crucial role in regional and global economic stability. As financial institutions in the UAE become more interconnected and reliant on digital systems, they increasingly find themselves targets for sophisticated cyberattacks. From ransomware and phishing to artificial intelligence (AI)-enabled manipulations, the cyber threat landscape continues to evolve, demanding innovative strategies to defend against these risks.

The ADGM Academy Research Centre recently published the Cyber Threat Report: The UAE Financial Sector Cyber Threat Landscape in collaboration with the Research and Innovation Centre of Rabdan Academy. The report provides insights from senior IT security managers at UAE financial institutions, aiming to enhance the understanding of current cyber threats and promote resilience in the financial sector.

To continue our exploration of cybersecurity we spoke to **Dr. Keri Pearlson, Executive Director of CAMS (Cybersecurity at MIT Sloan) and Advisory Board member of the ADGMA Research Centre**, where she shared insights on key themes regarding the threats facing the UAE’s financial sector. These include emerging threats, the role of AI, vulnerability management, and strategies for addressing advanced persistent threats (APTs) and supply chain vulnerabilities. Her analysis provides a blueprint for how financial institutions in the UAE can fortify themselves in this challenging environment.

Emerging Cybersecurity Threats: The Challenge of Ransomware, Phishing and AI Manipulation

The UAE's financial sector faces numerous cyber threats, with ransomware, phishing, and AI-facilitated manipulations being at the forefront. Each of these threats presents a unique set of challenges that can severely disrupt operations and tarnish the reputation of financial institutions.

Ransomware, which involves malicious actors encrypting critical data and demanding payment for its release, has become a highly effective tool for cybercriminals.

The UAE has seen a significant increase in ransomware attacks, largely due to the rapid digitisation and interconnectivity of its financial systems.

Phishing and spear-phishing attacks, where cybercriminals impersonate legitimate entities to trick individuals into divulging sensitive information, have become more sophisticated. AI tools allow these attacks to be customised, with emails appearing more realistic than ever. Pearlson notes that modern phishing emails are not the poorly written, easily identifiable scams of the past. Instead, they are targeted, well-crafted, and increasingly difficult to detect.

Finally, AI-facilitated manipulations, such as deepfakes and voice clones, pose an existential risk to financial institutions. Deepfakes involve the creation of realistic but fabricated video or audio content that can be used to impersonate executives or even conduct fraudulent transactions. Pearlson explains that these AI-powered tools are no longer just theoretical; they are being actively used by cybercriminals to manipulate and defraud individuals and companies.

Resilience: A New Mindset for Cybersecurity

In response to these growing threats, Pearlson advocates for a cybersecurity strategy centred around resilience. Rather than focusing solely on keeping cybercriminals out, she encourages organisations to build resilience into their operations, ensuring they can respond quickly and effectively to breaches when they inevitably occur.

Resilience, as defined by Pearlson, is the ability of an organisation to absorb shocks and return to normal operations, potentially stronger than before. This approach recognises that no matter how advanced defenses become, attackers will find ways to infiltrate systems. The real test lies in how quickly and effectively a financial institution can respond, recover, and continue operations.

“Resilience is a mindset,” Pearlson explains. “It’s not just about keeping the bad guys out but ensuring that If they get into your operations, you have built technological and organisational mechanisms so you can get back up and running quickly.”

For the UAE’s financial sector, resilience must extend beyond technology. Backing up data is critical, but as Pearlson warns, simply backing up systems without ensuring that the malware has not also been backed up can lead to further problems. Building resilience involves a holistic approach that includes testing backup systems, conducting regular incident response drills, and training staff on how to act during a cyber crisis.

One example she offers is tabletop exercises, where senior executives simulate a cyber breach and practice their response. These exercises not only prepare the technology and processes but also help develop the organisational muscle memory needed to respond to an attack swiftly. By simulating various attack scenarios - including ransomware, phishing, and AI-manipulated breaches - organisations can fine-tune their responses and improve overall resilience.

Pearlson also highlights the importance of communication planning in cyber resilience. She urges financial institutions to develop comprehensive cyber crisis communication strategies, including contingency plans for situations where normal communication channels, such as email, are unavailable due to a breach. Institutions should pre-determine who will communicate with different stakeholders (e.g., the public, customers, shareholders, and regulators) and what the general tone and content of the messaging will be. A well-planned cyber communication strategy for all stakeholders can mitigate the damage to a company’s reputation, reduce unintended consequences, and reassure stakeholders that the situation is under control.

AI’s Dual Role in Cybersecurity: A Game of Chess

Artificial intelligence is rapidly transforming the cybersecurity landscape. According to Pearlson, AI has a dual role—it can both enhance cybersecurity defenses and be exploited for more sophisticated attacks. This dynamic makes the cybersecurity battle akin to a game of chess, where both the defenders and the attackers use AI to outmanoeuvre each other.

AI’s positive role in cybersecurity includes its ability to improve efficiency, scalability, and visibility. AI tools can automate repetitive tasks, analyse vast amounts of data, and detect patterns that would be invisible to the human eye. For example, AI can help monitor network traffic, detect anomalies, and flag suspicious activity in real time, allowing financial institutions to respond more quickly to potential threats.

AI can also be used to help build resilience within organisations. Pearlson states that AI can aid in creating personalised learning experiences for employees. When an employee clicks on a test phishing email, for example, AI-driven tools can automatically generate a short training module tailored to that individual’s learning style and past behaviours. This approach can help ensure that employees are continuously learning and improving their cybersecurity skills.

However, AI also amplifies the threat. Cybercriminals are leveraging AI to make phishing emails more convincing, automate attacks, and even create deepfakes and voice clones. These AI-driven manipulations make it more challenging for employees to identify threats, increasing the likelihood of successful attacks.

One of the more concerning trends is the rise of AI-generated deepfakes. Deepfakes can be used to create realistic video or audio of a senior executive instructing a subordinate to transfer funds or share sensitive information. If employees are not trained to recognise these threats or to properly question unusual requests, a financial institution could be compromised.

Pearlson emphasises that organisations must be proactive in defending against AI-driven threats by educating employees, implementing verification procedures for unusual requests, and investing in AI tools that can detect and counter these attacks.

Vulnerability Management: The Human Factor

Vulnerability management is often viewed through a technical lens, with a focus on patching software and fixing bugs. However, Pearlson stresses that vulnerability management must consider the human element. Many vulnerabilities arise from the actions (or inactions) of employees, whether through phishing, poor password hygiene, or unintentional exposure of sensitive information.

Organisations must work to build a strong cybersecurity culture, where employees understand their role and know what to do to protect the organisation from cyber threats. Pearlson explains that creating a cybersecurity culture involves instilling **values, attitudes, and beliefs** that drive secure behaviours. Training programs alone do not work. Further, it’s not enough to simply tell employees not to click on suspicious emails; organisations must build an environment where leaders set the example, and employees feel responsible for their actions. Ideally everyone is motivated to do what is necessary to keep the organization secure, such as reporting suspicious activity.

One approach Pearlson recommends is using positive reinforcement. By recognising and rewarding employees who exhibit good cybersecurity practices, organisations can encourage others to follow suit. Some financial institutions issue “cyber hero” badges or other rewards to employees who report phishing attempts or successfully avoid falling for scams. This method of using carrots (rewards) instead of just sticks (punishments) can be more effective in fostering a proactive cybersecurity culture.

At the same time, there must be consequences for repeated failures. Pearlson shared the example of a company that implemented a progressive disciplinary system for employees who repeatedly clicked on phishing emails. After the third offense, employees would meet with their manager; after the fifth, they could be terminated. This system underscores the importance of taking cybersecurity seriously while allowing for initial mistakes to be corrected.

Advanced Persistent Threats (APTs): The Power of Information Sharing

Advanced Persistent Threats (APTs) pose a significant challenge to financial institutions in the UAE. These are often state sponsored, highly sophisticated attacks that are difficult to detect and can persist within an organisation's network for long periods before being discovered.

Pearlson highlights information sharing as a key strategy for combating APTs. In many countries and business sectors Information Sharing and Analysis Centers (ISACs) have proven effective in helping organisations share intelligence about emerging threats (e.g. FS-ISAC for financial services). For the UAE's financial sector, creating similar structures could be instrumental in staying ahead of cyber adversaries.

The reluctance to share information stems from concerns over reputational damage and fear of losing customers. However, Pearlson argues that by failing to share information, financial institutions are inadvertently allowing threats to proliferate. She stresses that the bad actors are already sharing information on the dark web, and financial institutions must find a way to do the same, albeit in a more secure and structured manner. “We need to be better than the bad guys at sharing information,” says Pearlson.

Information sharing can also lead to collective defence strategies, where financial institutions collaborate to develop new tools and technologies to detect and mitigate APTs. By pooling resources and intelligence, institutions can better protect themselves from long-term cyber threats.

Securing the Information Supply Chain: Managing Third-Party Risks

Financial institutions in the UAE are increasingly reliant on third-party vendors for critical services. This interconnectedness creates vulnerabilities in the information supply chain, where a breach in one vendor's system could cascade across the entire network.

Pearlson advises financial institutions to adopt a zero-trust approach when dealing with third-party vendors. This involves continuously verifying the security practices of vendors and ensuring that they adhere to the same cybersecurity standards. Regular audits, real-time monitoring, and contractual agreements that hold vendors accountable for their security practices can help reduce supply chain risks.

Moreover, Pearlson points out that supply chain attacks can be particularly damaging because they often go undetected for long periods. A vendor might be compromised months before the breach is discovered, giving attackers ample time to move laterally within the network. By the time the breach is uncovered, the damage may already be done.

To mitigate these risks, financial institutions must work closely with their vendors to ensure that the entire ecosystem is secure. Security must be a priority at every level of the supply chain. This can mean performing regular penetration tests and risk assessments and working with vendors to understand their own incident response plans. "The new mindset is that the entire ecosystem is working together to make sure everyone is resilient to a cyber event," explained Pearlson.

Building A Cyber-resilient Future

The future of cybersecurity in the UAE financial sector lies in building resilience, leveraging AI for defence, and fostering a culture of cybersecurity awareness. Pearlson's insights make it clear that technology alone is not enough to protect financial institutions from the ever-evolving threat landscape. A holistic approach—combining people, processes, and technology—must be at the heart of any effective cybersecurity strategy.

By focusing on resilience, financial institutions can ensure that they are not only prepared to defend against cyberattacks but also able to recover quickly and continue operations when breaches occur. Leveraging AI to enhance both defenses and employee training will further strengthen these efforts. Most importantly, by cultivating a culture where employees are motivated to act as the first line of defence, financial institutions can reduce the likelihood of human error and create a more secure operating environment.

As cyber threats continue to evolve, so too must the strategies that protect the UAE's financial sector. Pearlson's call for resilience is a reminder that while the battle against cybercrime may be ongoing, with the right mindset and tools, financial institutions can continue to thrive in a digital world.

ADGM Academy
Research Centre

Follow / Contact Us:

www.adgmacademy.com

✉ research@adgm.com

in LinkedIn