CYBER SECURITY & FINANCIAL INSTITUTIONS

CYBERSECURITY - THE EVER WIDENING SCOPE

Emerging technologies and an increase in sophisticated attacks indicates that financial institutions, a critical section of the UAE's vital infrastructure, continue to remain a main target for cyber attackers.

Despite the increase in cyber security spending over the past years, sensitive information is still at high risk of exposure. As the industry goes digital to meet consumer demands, each digital door (mobile apps, walk-in digital centers, banking robots, cloud, etc.), opens up new vulnerabilities and risks.

Extortion-based cyber attacks against financial institutions are on the rise and this guidance is intended to help financial institutions mitigate the significant risks posed by cyber attacks involving extortion, which include damage to an institution's liquidity, capital, operations, access to data and ability to provide services to customers and employees.

Two days before Christmas, Andrew, a server administrator with a regional bank, got an email purportedly from a credit bureau. A week earlier, he had applied for a car loan but he needed a credit report. Unsure about how to get one, he took to one of the popular public car forums and made enquiries.

David, a social engineer, notorious for crawling through car forums and spear-phishing unsuspecting forum members, came across Andrew's enquiry. He sent Andrew an email with an attachment and subject "*Credit Report for your Car Loan*". A click on the attachment was all that was required.

David bypassed all existing controls, obtained administrator access to Andrew's system and the bank's payment system. Over 150,000 customers' details were compromised.

> “A click on the attachment was all that was required. David obtained administrator access to Andrew's system and the bank's payment system. Over 150,000 customers' details were compromised.”

BDO UAE TECHNOLOGY ADVISORY

BDO UAE's Technology Advisory practice consists of seasoned technology advisors who come from diverse backgrounds and cover a range of specialist skill sets in: Cybersecurity, IT Audit, Governance, Risk and Compliance(GRC), Forensics and Security Awareness and Training. Our passion is to see organizations extract the best value from a resilient and secure technology environment.

CONTACT US:

RICHARD UHUNMWAGHO
Manager
Technology Advisory Services

Tel: +971 4 436 3500
Mobile: +971 55 810 7750
richard.uhunmwagho@bdo.ae

BDO Chartered Accountants & Advisors
www.bdo.ae

Cyber-attackers target financial institutions for various reasons; (a) ransom ware attacks; (b) Denial of Service (DoS) attacks; (c) attacks involving theft of sensitive business or customer information, with perpetrators threatening companies with the information's public release. These attacks have an effect on an institution's base line and reputation. It can be expensive, damaging to client confidence, and, in various cases, the bank might be held officially responsible.

Ensuring a sustainable cyber-resilience is not just about preventing employees from clicking links or installing anti-phishing tools across the network but having to take a broader, intelligence-based approach in mitigating risks posed by systems (legacy and emerging technologies), human error and deliberate attacks on their organization.

#BDOKNOWS Cybersecurity: Financial Institutions & Recommendations

- Conduct ongoing information security risk assessments using a repeatable methodology that integrates business processes, impact analysis and controls selection.
- Map out the bank's most business-critical parts of the network and use network segmentation as a strategy. This limits the ability for a hacker to move laterally across a compromised network.
- Provide mandatory trainings to employees at all levels (from top management to junior management) about cyber security at an ongoing basis.
- While regulatory compliance (NESA, ISO 27001, PCI etc) is important, a compliant environment is not necessarily a secure one. The sharing of information about cyber threats and vulnerabilities with other banks, IT security firms and government agencies in real-time should be encouraged by regulatory bodies.
- Ensure data security events are analyzed and interpreted in real-time. This can be achieved either through in-house cognitive security technology deployment or by contracting a third party to manage user behavior analytics, security monitoring and incident response for your bank.
- Conduct frequent tests of your cyber defense; track adherence to security processes, procedures & controls; monitor employee's system habits; and embed security into the DNA of your business – products, services and people.

For more on cyber security services provided by BDO, please visit our page on:
http://www.bdo.ae/en-gb/services/advisory/technology-advisory-services/cybersecurity-services