CYBERSECURITY

WITH A VIEW TOWARDS RISK AND LIABILITY REDUCTION

BY MICHELLE GARCIA GILBERT
MANAGING PARTNER,
GILBERT GARCIA GROUP, P.A.

WHERE ARE WE?

Default service professionals handle large amounts of personally identifiable information (PII) in the course of their work. Security breaches involving PII have led to individuals falling victim to identity theft, embarrassment, and blackmail; organizations have suffered a loss of public trust, legal liability, and increased remediation costs. [2]

TARGET, DECEMBER 2013

AROUND

40 MILLION

DEBIT AND CREDIT CARD ACCOUNTS EXPOSED DURING HOLIDAY SEASON

U.S. OFFICE OF PERSONNEL MANAGEMENT, JUNE 2015

OFFICE REPORTS

21 MILLION

SOCIAL SECURITY NUMBERS WERE STOLEN IN 2014

SONY, NOVEMBER 2014

FBI REPORTS NORTH KOREA HACKED

PERSONAL INFORMATION ON CELEBRITIES (I.E., SYLVESTER STALLONE) AND EMPLOYEES GOING BACK SEVERAL DECADES

ASHLEY MADISON, JULY 2015

HACKERS RELEASED

INFORMATION ON MILLIONS

OF PEOPLE WHO USED THE MARRIED DATING SITE AFTER THE COMPANY REFUSED DEMANDS TO SHUT DOWN THE SITE

[2] Government Accountability Office (GAO) Report 08-343, Protecting Personally Identifiable Information, January 2008, http://www.gao.gov/new.items/d08343.pdf

EQUIFAX, SEPTEMBER 2017

AS MANY AS

143 MILLION

AMERICANS' PERSONAL INFORMATION WAS EXPOSED

FACEBOOK, SEPTEMBER 2018

BETWEEN JULY 2017 AND SEPTEMBER 2018, HACKERS

ACCESSED

INFORMATION

OF ABOUT

30 MILLION USERS

UBER, NOVEMBER 2017

UBER PAID

$100,000

TO HACKERS IN 2016 TO TRY TO MINIMIZE BREACH OF INFORMATION FOR 57 MILLION RIDERS AND DRIVERS

MARRIOTT/STARWOOD, NOVEMBER 2018

AS MANY AS

500 MILLION

STARWOOD GUESTS HAD INFORMATION EXPOSED SINCE 2014

YAHOO, OCTOBER 2017

VERIZON, AS OWNER OF YAHOO, REVEALED THAT ALL

THREE BILLION

YAHOO USERS'

INFORMATION

WAS HACKED IN 2013, THREE TIMES THE NUMBER REPORTED IN 2013

FIRST AMERICAN FINANCIAL CORPORATION, MAY 2019

AN ESTIMATED

885 MILLION

DOCUMENTS RELATED TO REAL ESTATE CLOSING DATING BACK TO 2003 WERE LEAKED, EXPOSING PERSONAL INFORMATION

Headlines report the activities of hackers and the prevalence of vulnerabilities of online data systems almost daily.[2] In 2015, the Federal Financial Institutions Examination Council (FFIEC) issued a Cyber Assessment Tool for use with financial institutions which come under the oversight of the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Association (NCUA), the Bureau of Consumer Financial Protection (BCFP), and the State Liaison Committee of State Regulators, all of whom are members of the FFIEC.[3] The assessment "…provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time." [4]

The Cyber Assessment Tool is a starting point for financial institutions to mitigate information security risks. However, complex business relationships require a thoughtful review of the entire business model. For independent mortgage brokers and loan officers, personal devices are commonly used which may cause vulnerability when dealing with personal information. In fact, the approach to cybersecurity risk reduction should be enterprise-wide and involve extensive information gathering.

Part of the problem is the identification of potential sources of PII utilized by a company and its vendors. Sources include databases, shared network drives, backup tapes, and contractor or vendor sites which contain PII, described as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[5]Best practice procedures

EXAMPLES OF PII INCLUDE, BUT ARE NOT LIMITED TO:

1. Name, such as full name, maiden name, mother's maiden name, or alias
2. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
3. Address information, such as street address or email address
4. Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
5. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

[2] Privacy Rights Clearinghouse, Office of Personnel Management; Facebook; Target; Marriott; *NY Investigates Exposure of 885 Million Mortgage Documents*, Krebs on Security, May 19, 2019

[3] https://www.ffiec.gov/cyberassessmenttool.htm

[4] Id.

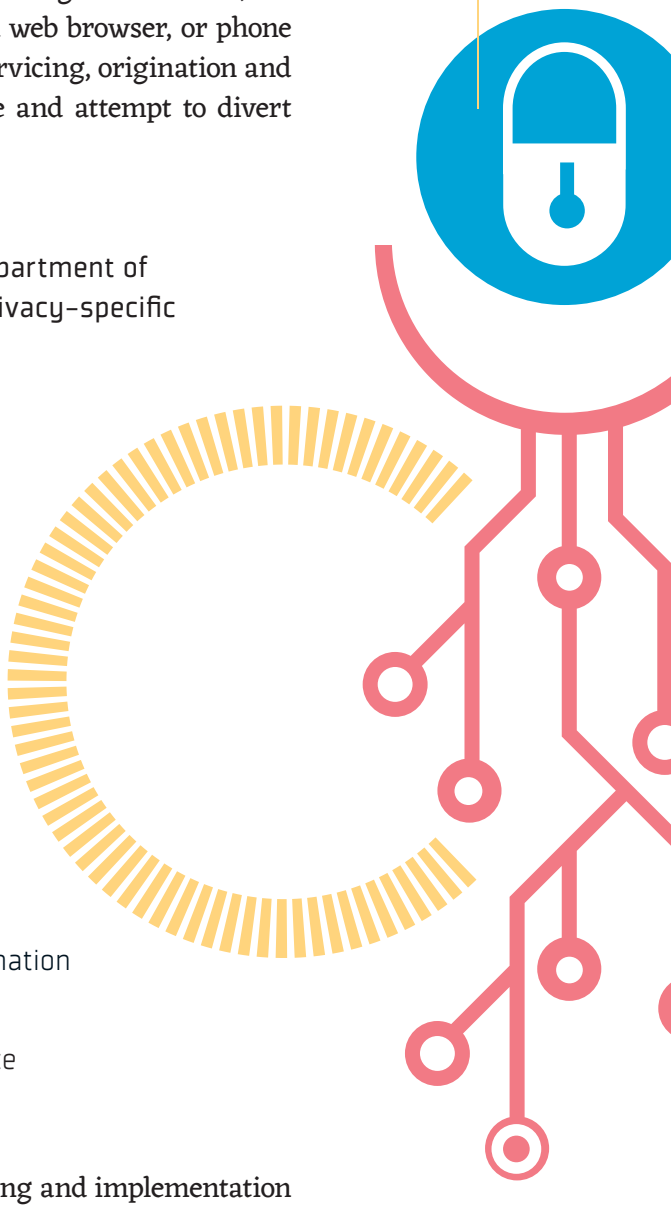
[5] OMB Memorandums 07-16 and 06-19. GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, http://www.gao.gov/new.items/d08536.pdf.

for handling PII abound among government agencies and private business, and merit mention in the context of default servicing professionals. Looking from the unique perspective of a potential hacker illustrates where a business should focus efforts, given that a thorough perimeter security (firewalls, patching protocol, etc.) is in place. Experts claim that up to 80% of system breaches occur by "social engineering."

Social engineering is the manipulation of people into performing actions or divulging confidential information. Some outcomes of social engineering include individuals or organizations sharing confidential information through phishing email scams, introducing malware by navigating to unsafe websites through a web browser, or phone phishing for sensitive information. Particularly in the default servicing, origination and mortgage lending industry, phishing emails appear legitimate and attempt to divert wires and payments to hackers.[6]

The National Institute of Standard and Technology (U.S. Department of Commerce) recommends using operational safeguards, privacy-specific safeguards, and security controls, such as[7]:

1. Creating Policies and Procedures
2. Conducting Training
3. De-Identifying PII- meaning confirming information must be encrypted
4. Using Access Enforcement
5. Implementing Access Control for Mobile Devices
6. Providing Transmission Confidentiality
7. Auditing Events
8. Developing Incident Response Plan to Handle Breaches
9. Requiring Coordination Among Teams, especially Information Technology, Human Resources and Operations
10. Confirming Adequate Cybersecurity Insurance is in Place



Two key and inexpensive protections stand out: employee training and implementation of software patches upon release. Given the proliferation of social engineering, employees should be informed daily about schemes, trained and tested on a frequent basis, and encouraged to report any and all cybersecurity incidents. Software patches address shortcomings in a developer's software; unpatched systems attract hackers who work at finding system vulnerabilities.

[6] Cybersecurity Best Practices in Mortgage Banking, Jim Deitch, Mortgage Compliance Magazine, http://www.mortgagecompliancemagazine.com/featured/cybersecurity-best-practices-in-mortgage-banking/

[7] NIST Special Publication 800-122, April 2010

WHAT CAN WE DO?

Some experts propose more federal and state regulation and oversight of cybersecurity, similar to the model of public utilities, public transportation, and the internet, but without the cooperation of the private sector, the expense of such a massive government undertaking is cos-prohibitive. The NIST has already developed a set of common cybersecurity standards based on accepted international criteria which can set the stage for solutions implemented by all stakeholders, public and private. One downside of too much government intervention stems from a one-size-fits-all mentality; in a cyber world diverse in functionality and purpose, one standard security method may lead to a false sense of security. A balanced approach might be best: government institutional oversight and promotion of best practices, combined with diversity, development, and redundancy from the private sector.[8]

Much of the private sector understands the risk of a lack of sound and responsive cybersecurity protocol: the always-changing landscape of cyber risk combined with exposure footprint of different companies can lead to disastrous results. Effective cyber risk management requires an integrative approach, including government regulation, in order to adapt to inevitable threats.[9]

WHAT IS ON THE HORIZON?

Experts and politicians warn that the current encryption protocol used in the United States will be hacked in the near future. A rising technology called quantum computing significantly reduces the time it takes to perform computations. Problems that required billions of years with non-quantum computers can be solved in a matter of days or even hours with quantum computing. "In quantum computing, a qubit (short for quantum bit) is a unit of quantum information—similar to a classical bit. Where classical bits hold a single binary value such as a 0 or 1, a qubit can hold both values at the same time in what's known as a superposition state. When multiple qubits act coherently, they can process multiple options simultaneously. This allows them to process information in a fraction of the time it would take even the fastest nonquantum systems."[10]

U.S. experts warn that our current ability to encrypt and secure PII within the next decade will be impossible with the advent of quantum computing, because quantum can unlock encryption. Currently, hacked data is indecipherable but may not be for long once quantum computing is fully functional. In fact, countries like China and Russia devote resources to the development of quantum computers, while U.S. researchers move as rapidly as possible to develop not only quantum computers but also the next wave of encryption before it is too late.[11]

While chair of the IT Subcommittee of the House Oversight and Reform Committee, Congressman Will Hurd from Texas advocated for modernization of the U.S. IT system and stated at the Aspen Security Forum on July 20, 2018, "Whoever gets to the true quantum computing first will be able to negate all the encryption that we've done to date."[12] Hurd recommends that a national coordinator for quantum computing be appointed within the White House.

The following diagram, a version of which was compiled by the Wall Street Journal based on data from IBM, NIST, and the Center for New American Security illustrates the situation.

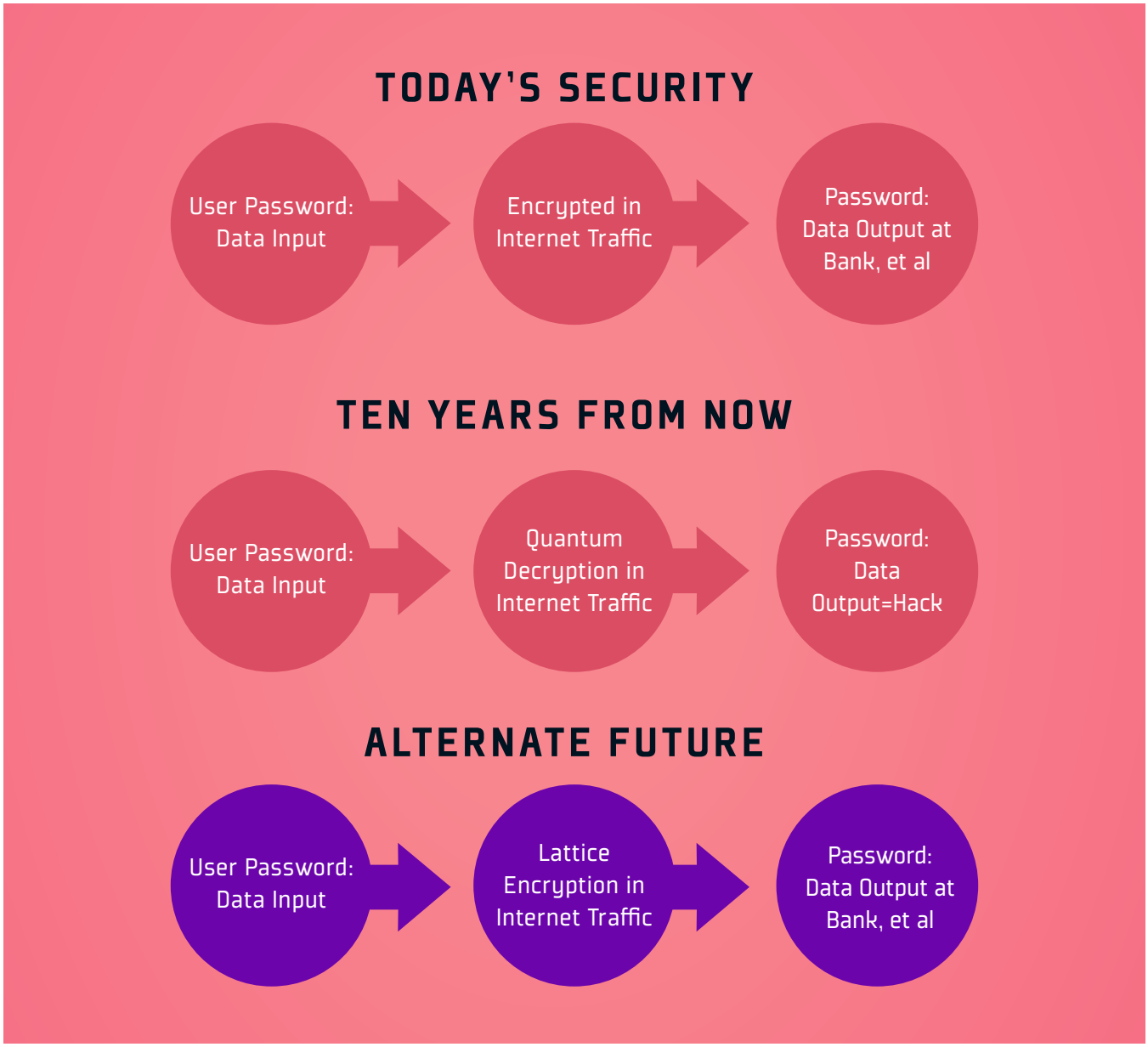
[8] *Should the Government Require Companies to Meet Cybersecurity Standards for Critical Infrastructure?* Wall Street Journal, November 18, 2018

[9] *Lack of Understanding is the True Cyber Risk*, Corporate Counsel Business Journal, May-June 2019

[10] https://www.microsoft.com/en-us/quantum/what-is-quantum-computing

[11] The Race to Save Encryption, Christopher Mims, Wall Street Journal, June 5, 2019, https://www.wsj.com/articles/the-race-to-save-encryption-11559646737

[12] https://hurd.house.gov/media-center/in-the-news/best-piece-legislation-dc-about-quantum-computing



Lattice encryption is a complex cryptographic scheme designed to protect data from the threat of crypto-breaking by quantum computers; in other words, it hides data inside complex math problems. Though quantum computing is still many years away, the use of lattice cryptography now and in the future thwarts hackers of all types.[13]

One downside is that older data can be hacked with quantum computers, and back actors are hacking and stockpiling data in order to decrypt it in the future. Another downside is the lack of a quantum-safe standard, but help is on the way.[14] No one knows exactly when quantum computing will be capable of hacking current encryption. The National Institute of Standards began a post-quantum cryptography standardization project in 2016, to be completed around 2022. Implementation of a standard may take five to ten years, so time is of the essence. Cybersecurity experts from Google, Microsoft, IBM, and the federal government are currently focusing on finding solutions, though those experts acknowledge the tremendous threat from China who has devoted considerable resources to quantum computing.

This macro view of maintaining the security of PII in default servicing and mortgage industry impacts the day-to-day efforts to prevent hacking and inadvertent exposure of PII. Industry participants should be informed about the future of cybersecurity on our work and should support private and public efforts to address future threats. W

[13] https://www.research.ibm.com/5-in-5/lattice-cryptography/

[14] The Race to Save Encryption, Christopher Mims, Wall Street Journal, June 5, 2019, https://www.wsj.com/articles/the-race-to-save-encryption-11559646737