The dangers of lending in a digital world: 2017 edition

Introduction

The mortgage lending industry is an ever-growing target for data thieves. Given the number of potential victims at risk, and the value of the data they hold, organizations that operate within the lending industry are sitting ducks for the criminals who seek to exploit them.

Worryingly, things look set to get worse before they get better: Increased adoption in web-based and mobile technologies in the workplace, exacerbated by the growing sophistication of cyber criminals, culminate in a level of threat that many lenders are struggling to deal with.

While it's easy to point to technology as the problem, in reality it's the people responsible for managing those technologies who should be placed under closest scrutiny. Lenders rely heavily on technology to function - the onus is on them to ensure those technologies are used responsibly, so that they do not become a gateway for unwanted guests.

An investigation into U.S. mortgage lenders undertaken in 2014[1] found that 70% of mortgage lenders may be putting sensitive data at risk through their application processes, by allowing applicants to submit personal and financial information via unencrypted email. The investigation concluded two key points: Firstly, there is a general lack of security knowledge among mortgage lenders; and secondly, lenders would sooner prioritize customer convenience over security.

The intention of this guide is to help mortgage lenders better understand cybersecurity, and the risks that exist in today's rapidly evolving landscape.

Reasons to be fearful

1. Financial services in top three industries affected by data breaches

The 2016 Data Breach Investigations Report by Verizon lists financial services in the top three industries affected by a data breach (an incident that resulted in confirmed disclosure to an unauthorized party) or security incident (any event that compromises the confidentiality, integrity, or availability of an information asset). While no industry is immune to security failings, the fact that financial services has also placed in the top three in previous editions of this report is no coincidence.

Industry	No. Security Incidents	Confirmed Data Loss
Accomodation	362	282
Administrative	44	18
Agriculture	4	1
Construction	9	4
Educational	254	29
Entertainment	2,707	38
Financial Services	1,368	795
Healthcare	166	115
Information	1,028	194
Management	1	0
Manufacturing	171	37
Mining	11	7
Other Services	17	11
Professional	916	53
Public	47,237	193
Real Estate	11	5
Retail	370	182
Trade	15	4
Transportation	31	15
Utilities	24	7

Data taken from The 2016 Data Breach Investigations Report (DBIR) by Verizon.

2. The cost of data breaches is rising
According to IBM and Ponemon Institute's 2016 Cost of Data Breach Study, the average cost of data breach in the U.S. has increased by approximately 10% in three years:

Financial year	Average per capita cost of data breach
2014	$201
2015	$217
2016	$221

Source: IBM and Ponemon Institute's 2016 Cost of Data Breach Study

What's more, the average per capita cost of a data breach within the financial industry specifically is the third highest of all industries, at $221.

Industry	Average per capita cost of data breach
Health	$355
Education	$246
Financial	$221
Services	$208
Life Science	$195
Retail	$172
Communications	$164
Industrial	$156
Energy	$148
Technology	$145
Hospitality	$139
Consumer	$133
Media	$131
Transportation	$129
Research	$112
Public	$80

Source: IBM and Ponemon Institute's 2016 Cost of Data Breach Study

3. Cyberattacks are becoming increasingly sophisticated
There is much evidence to suggest that cyberattacks are becoming more technically sophisticated, as the criminals who look to infiltrate organizations seek new ways of outsmarting equally sophisticated security systems.

If you asked someone to picture a cyber criminal, they would most likely conjure up an image of a lone amateur operating from their basement: while such individuals do exist, at the other end of the spectrum exists highly organized teams of cyber criminals, who operate in broad daylight, mirroring the organizations they seek to exploit. The modern cyber criminal is highly skilled and should not be underestimated.

Understanding the threats

Lenders need to familiarize themselves with the types of data breach that they may come up against, understand how they occur, and know how to prevent them.

Data breaches very rarely occur at a single point in time, but are more commonly part of a complex chain of events. Organizations must mitigate all possible paths an attacker can take, not just the direct path from point A to point B.

Even organizations that maintain robust in-house security policies could be at risk through association of their third-party vendors. While your organization may deploy highly sophisticated cybersecurity standards, if your vendors have weak systems or controls, those protections may be rendered ineffective. Therefore the onus is on you to ensure any third-party tools, software, or services utilized by your organization meet sufficient security standards.

The increase in the use of mobile devices and BYOD (bring your own device) in the workplace has added to the risk of breaches, and lost and stolen devices pose a huge threat; particularly if devices are not encrypted or password protected. To minimize risks, user authentication should be multi-tier, sensitive data should be encrypted, and documents and data should only be shared within secure environments.

Human error still poses the biggest risk of all
When it comes to cybersecurity failings, humans are consistently the weakest link in the chain. A report by Kroll suggests that human error can be blamed for around 60% of breaches[2] within organizations.

Employee negligence, such as disposing of sensitive information improperly, accidents, like a member of staff posting a link to data outside of a secure network in error, and poor training resulting in staff using weak passwords, have all been revealed as reasons behind past data breaches. This is not to mention the threat of employees who intentionally put organizations at risk for their own benefit. While such cases may be rare, it is extremely difficult to safeguard against internal threats when they are malicious in nature.

A culture of security

For organizations at the larger end of the scale, the Chief Information Security Officer (CISO) is typically the person responsible for establishing and maintaining cybersecurity standards. Within smaller organizations, this responsibility may sit with the IT department, senior management, or elsewhere. Regardless of an organization's size and structure, cybersecurity should not be one person's sole responsibility, but that of the entire organization.

By developing a "culture of security" throughout an organization, including regular staff training and knowledge sharing sessions, the risk of data being leaked or stolen as the result of human error will be significantly reduced. Further still, businesses should ensure all employees sign a declaration stating they understand the businesses security policies, their responsibilities as an employee, and the penalties associated with non-compliance.

While every effort can and should be made to ensure technologies are secure and adhere to laws and industry regulations, these efforts are worth nothing if the people using the technologies fail to follow suit. The fact is, no breach is unavoidable, and businesses that have fallen victim to attack or have leaked sensitive information inadvertently, have no one to blame but themselves.

Your responsibilities

As a lender, the Consumer Finance Protection Bureau (CFPB) and the Graham Leach Bliley Act (GLBA) require you keep your customers' information protected. Now that TRID has been fully implemented, there is renewed interest in CFPB audits, and with the threat of data breaches looming every day, auditors are keeping a close eye on adherence to the rules around the privacy and security of customer data.

Major regulations and laws that should be reviewed by your legal and compliance teams to ensure your organization complies include the following:

Gramm-Leach-Bliley Act [Section 501(a) and 501(b)]
Information Security Breach Notification Legislation
Identity Theft Red Flags Rule
Security Federal Financial Institutions Examination Council (FFIEC) Guidelines
Federal Trade Commission (FTC) Regulations
Federal Deposit Insurance Corporation — PR-28-2014
SEC Cybersecurity Guidance
New York State Department of Financial Services (NYS-DFS)
OCC Bulletin 2013-29
CFPB Bulletin 2012-03
Federal Reserve — Guidance on Managing Outsourcing Risk (SR letter 13-19 / CA letter 13-21)

All organizations should develop an information security program to manage risks inherent in the use of technology. These risks, and the need to effectively manage them, exist regardless of any laws or regulations. Failure to manage these risks can have catastrophic consequences, from ruining long-standing customer relationships, through to legal penalties.[3]

As well as federal laws, the majority of states have their own laws pertaining to data breaches[4]. Fines and consequences can therefore vary depending on the severity and type of breach, as well as where the breach occurred.

The fundamentals of an information security program

Every organization should maintain a robust information security program. The MBA (Mortgage Bankers Association)[5] offers some great advice for lenders looking to implement an information security program of their own. For this, The MBA recommends organizations follow a two step implementation process, starting with the implementation of 13 key first priority practices (including risk management, firewall installation and employee training), and followed up with 14 second priority practices (including encryption, BYOD security and disaster recovery planning). While the recommended practices are categorized into either first and second priority, none should be discounted.

The future of lending in a digital world

"There's a new level of sophistication going on out there in cyber threats."

- Jessica Edgerton, Associate Counsel, National Association of REALTORS®

The sheer volume of data breaches reported every year shows that even large organizations who spend vast amounts of money on information security can be vulnerable, and no matter how good the security strategy, there can still be gaps. Cyberattacks are not only on the rise , but are becoming increasingly sophisticated and will continue to evolve.

The evolution of technology means IT departments more than ever have to find secure ways of supporting new devices and platforms, meaning that organizations are being exposed to new risks on a daily basis.
Organizations must evolve constantly too. No matter how small or large, mortgage lenders cannot afford to be complacent because no organization is immune to a data breach. Information security is too important not to be given due consideration, and the threats against the industry look like they will only continue to escalate. In what is essentially an ongoing game of cat and mouse, it must be the lenders who set the pace, and not the criminals who seek to exploit them.

We are XDOC

AXACORE has been highly successfully in helping our lending customers improve their document workflow while making it easier to capture, manage, find, classify and deliver loan documents. AXACORE delivers value to the lending industry on premises and cloud versions of XDOC electronic document management for mortgage lending. XDOC improves productivity and lowers costs by taking paper based processes out of the equation so lenders can close more loans with less clicks.

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports