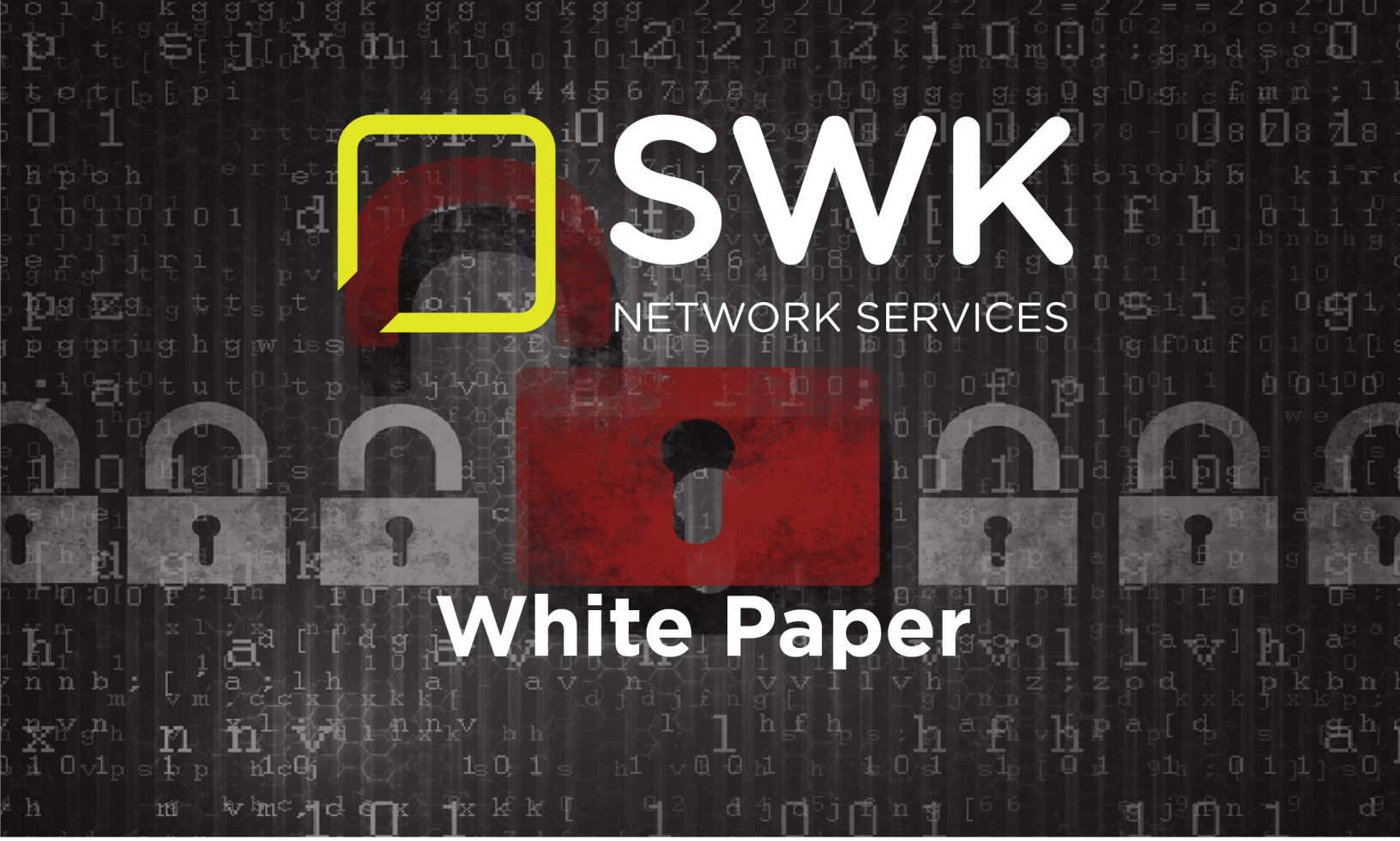


Common threats to the Title Insurance Industry and how to prevent them

By: Hector Bonilla
SWK Technologies

West Deptford, NJ • East Hanover, NJ
Phone: (856) 956-5800 • nwsinfo@swktech.com
www.swknetworkservices.com

SWK NETWORK SERVICES

Contents

The title insurance industry is experiencing an era of significant change coinciding with the emergence and deployment of many new technological tools within the greater financial sector and beyond. The widespread adoption of the Internet and digital applications provide considerable opportunities to improve communication and connect parties separated by otherwise insurmountable circumstances. However, it also creates many unintended vulnerabilities as networks continue to expand more rapidly than their hosts can contain them. The transition of commerce to online portals and digitization of personal information has made data extremely valuable, especially to commercial enterprises and to cybercriminals. Both groups increasingly rely on data being exchanged to generate profitability, but the latter work solely to exploit the owners of this information to extract a short-term return through illicit means.

As a subsector of finance, title insurance is a prime target for hackers seeking to expropriate some or all of the monetary transactions being made over digital channels constantly. Attackers have amplified the amount of effort they devote to identifying and entrapping targets to improve whatever gains they can siphon from a successful network breach. They especially focus on industries that rely on sizable commercial transactions and use social engineering tactics to build profiles on the personnel that manage these exchanges. Regulatory agencies like the Federal Trade Commission (FTC) are recognizing that scammers use electronic communication to insert themselves into real estate negotiations at critical junctures using well-researched email phishing methods that can fool people into turning over large one-time monetary transfers or even their whole accounts to hackers.

Several consumer privacy laws in the U.S. are being redefined to incorporate the expanding importance of digital information and new legislation is appearing that focuses solely on network security within certain industries. Title agencies must commit to a balancing act of adopting technology to remain competitive while also addressing the additional pain points these tools create. To ensure sustainability, title insurance businesses have to refocus on cybersecurity not just to comply with regulations, but also to defend the increasingly valuable data they rely on to operate effectively. An extensive IT security strategy will both meet compliance and help ensure protection against the many cyberthreats that exist today. SWK Network Services is an award-winning Managed Service Provider that delivers premium network security solutions that enable title insurance agencies to meet their industry compliance obligations.

Finance

Financial institutions require comprehensive cybersecurity solutions in order to maintain their commercial and regulatory obligations, and this need will only grow as digital technology takes over the industry. Online commerce allows services to be streamlined and to be facilitated with faster deliverables. Electronic communication bridges the distance between parties so that transactions can be completed across the globe. The amount of data that must be exchanged to facilitate these operations every day can be substantial and provide a tempting target to cybercriminals.

Technology

The title insurance sector is positioned to greatly benefit from the introduction of new digital tools that significantly improve client experience and engagement. Alternatives such as e-closing provide new opportunities not fulfilled by traditional methods. Taking advantage of applications that include digital documentation and signatures, video conferencing and online portals allows title agencies to simplify the closing process and complete contracts faster and much more conveniently for the client.

Though larger insurance entities continue to focus on mergers and acquisition to spur growth, research[1] has shown that smaller agencies are well-situated to deploy technology to stand out among competitors. Digital applications are set to disrupt the title insurance industry within the coming years as new technology offers agents the opportunity to enhance their processes.

Qualia, a platform that streamlines the closing process and is designed for deployment in title insurance transactions, has already managed to captured five percent of the national real estate market since its inception in 2015[3]. Pavasso, another e-closing solution launched in 2014, is being increasingly adopted by larger, well-established title agencies, including Title Source and Old Republic National Title Insurance Company[4]. Agencies that have existed for over a century are now turning towards digital applications less than a decade old to maintain their positions in the market.

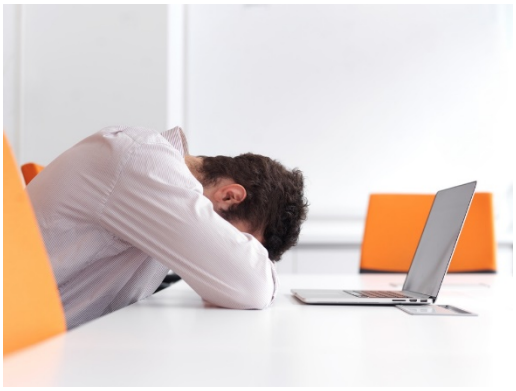
Threats

Digital transformation does not come without risk and any organization connected to the Internet has some level of exposure. A report by cybersecurity firm Digital Shadows[2] estimates that approximately 1.5 billion data files have been leaked onto the web at one point or another, with almost 240 million of those originating in the U.S. alone. These include credit card numbers and other pieces of financial information.

There are several threats that are universal to every network and some that are deployed against title agents and other financial service professionals specifically. The most common danger is malicious software, which is most often delivered through phishing emails or websites. Understanding these threats is often the first step towards protecting against them:

Human Error

Nearly every cyberthreat relies on a lack of user awareness to succeed. Phishing emails and dummy websites rely on an individual dropping their guard long enough to click on a link that will download malware onto the machine they are operating. Human error is the most efficient vector for penetrating a network and mining the data within the connected system.



SWK Network Services' Phishing Defender solution is a comprehensive employee security awareness training program that is proven to reduce the likelihood of an employee falling for a phishing scam. You will gain access to testing, compliance reporting, even strategic training for specific departments and other resources that will enable you to both improve your cybersecurity and fulfill federal and industry best practice requirements.

Wire Transfer Fraud

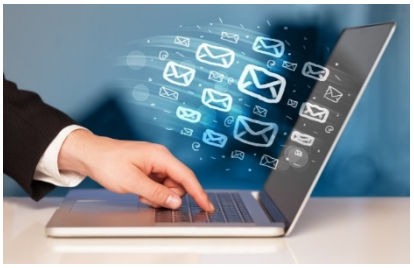
By far the most potentially damaging threat to title agents is wire transfer fraud[5]. An attacker will send a message masquerading as a trusted party expecting to receive payment and will submit instructions for wiring the funds. The thieves may employ incentive to impart a sense of urgency upon their victims to transfer the money without investigating further. Often, they are based overseas and rely on the inability of law enforcement to trace the transaction across international systems.

Hackers will initiate wire fraud schemes by gaining access to the confidential communications of title agents and their partners, customers and other involved parties. Title agencies can prevent attackers penetrating their networks by employing an email encryption solution that delivers enhanced message security.

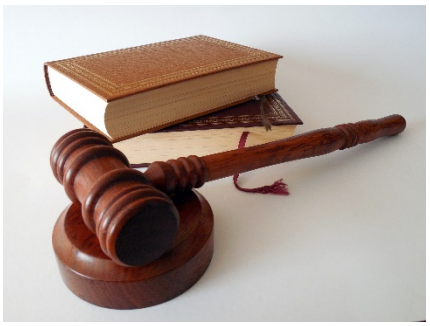
Ransomware

Ransomware can affect businesses of all sizes in many different industries, but it presents the greatest threat to those who store sensitive data and to those who rely on their digital information to deliver value in a timely manner to clients. Successful breaches can also signal network vulnerabilities that can lead to worse outcomes. Hackers that deploy ransomware rely on desperation resulting from the victim being locked out of their system and unable to access critical files contained therein.

A strong business continuity solution is key to defending against ransomware attacks. However, not just any backup solution can provide this kind of protection. SWK Network Services is able to provide a custom backup and disaster recovery solution that is designed according to your needs to allow your business to continue running smoothly.



Legal Guidelines



The rising prominence of cyberthreats and the increasing impact they have on protecting NPI is leading to reevaluations of existing digital privacy laws that affects industries such as real estate and finance. As title insurance exists at a junction between both of those sectors, it is subject to a wide array of regulatory obligations. Maintaining compliance entails knowing the requirements of each of these laws and understanding how they might be affected in the future.

Financial Regulations

Legal requirements regarding NPI in the financial sector have had to be reviewed and reassessed as digital communication technology has evolved. Current amendments are building upon mandates that were mostly established at the turn of the new millennium. Legislation regarding digital NPI has followed a pattern of becoming more stringent in response to the amount of data being processed and the discovery of vulnerabilities.

Federal Regulations

There are several federal regulations concerning the protection of NPI belonging to consumers that affect financial institutions. Chief among these are the Privacy of Consumer Financial Information Rule (Financial Privacy Rule) and the Standards for Safeguarding Customer Information (Safeguards Rule) of the Gramm-Leach-Bliley Act (GLB Act) of the FTC. Even if an organization is not technically a financial institution, collecting financial NPI from consumers can place them under the jurisdiction of the Act. This legislation creates general disclosure and privacy obligations for organizations that manage such data and stipulates that they create security processes to protect it.

Local & State Regulations

Digital NPI regulations have also emerged from local and state government agencies that address new and developing realities of modern cybersecurity. The New York Department of Finance established 23 NYCRR 500 (Part 500) to enforce network security requirements among financial institutions operating within the state of New York. It lays down similar rules to those of the GLB Act, but creates more specific and proactive obligations for safeguarding financial data.

One of the most critical of these new requirements is the implementation of a comprehensive internal network security audit. Part 500 mandates that financial entities gain an accurate measure of their cybersecurity processes to help ensure their protections are adequate. These assessments must be completed at regular intervals by either an internal IT staff or an experienced third party. SWK Network Services can enable title agencies to meet compliance with Part 500 by deploying our Network Vulnerability Test solution, which allows you to gain a full understanding of the state of your cybersecurity practices.

International Regulations

The European Union passed the General Data Protection Regulation (GDPR) in as a sweeping NPI compliance legislation that affected all EU citizens. It builds off of regulations established in previous

decades similar to the trends with data protection laws in the US, however, it accomplishes significantly more in scope. It effectively redefines NPI as the property of the individual who it initially belongs to and creates stricter requirements of commercial organizations for acquiring, managing and safeguarding personal information. It also expands compliance requirements beyond the EU's borders to any enterprise that actively markets to EU citizens.

The GDPR has deeper ramifications in the precedent it sets for data protection legislation. It expands the nature of NPI to include all data that can be used to identify an individual person as well as significantly elevates its importance under the law. The GDPR acts as a more extensive and thorough version of previous rulings regarding information privacy and may establish a model for future regulations to follow.

ALTA

The American Land Title Association (ALTA) represents over 6000 title agents, underwriters and abstractors and has at least one active member in every county in the United States. ALTA documentation and policy establish a common national standard for title insurance agencies across the country. There are several ALTA best practice "Pillars" that effectively enhance the existing obligations of title agencies as financial institutions and insurance brokers to complying with government regulations.

Pillar 3

Pillar 3 of the ALTA Title Insurance and Settlement Company Best Practices is the most comprehensive and compliance-intensive of the ALTA best practices list. It mandates that title agencies must primarily adopt and maintain a written privacy and information security program to protect NPI according to the requirements of local, state and federal law, among other stipulations. These include establishing physical and network security systems for NPI, proper information disposal procedures, creating a disaster management plan, providing training and oversight for employee compliance processes, self-auditing and review of security programs, and notifying customers and law enforcement of security breaches.

Instances of noncompliance regarding certain components of Pillar 3 can cause title agents to fail ALTA certification procedures for an individual occurrence. Combined with the added obligations it places on compliance with other regulations, Pillar 3 induces an increased burden of responsibility for title insurance agencies to safeguard customer NPI. However, agents who do demonstrate consistent compliance can receive documentation of their certification for use with their client engagement, which will also corroborate their continued adherence to government regulations as finance and insurance professionals.

Security & Compliance

Title insurance professionals face a two-pronged situation in determining how to develop a comprehensive security program that will both safeguard their data and fulfill the requirements of regulatory bodies. As the industry experiences improving margins, title insurance transactions may become more enticing targets for hackers. Coupled with a shifting legal landscape, an overview of cybersecurity for title agent contracts is increasingly necessary.

A majority of cyber attacks are initiated by phishing campaigns or another method of deceiving the victim in a way that prompts them to lower their guard and unwittingly leak critical identification data. Preventing these types of penetration attempts from being successful in the first place requires a defensible system and the proper training to identify the initial signs of an impending hack.

We make it our goal to provide you with comprehensive IT solutions that allow you to control network costs and maintain security compliance. SWK's cybersecurity services enable our clients to consistently and proactively meet modern network security standards and best practices. Contact us to find out more about how our managed service solutions can help you streamline your digital security regulations compliance processes and safeguard your network.

1) "U.S. Insurers Seeking Scale By M&A, Differentiating by Technology" Forbes, 2018.
2) "Too Much Information" Digital Shadows, 2018.
3) "Qualia Grabs $33M Series B Led by Menlo Ventures to Simplify the Home Closing Process" Forbes, 2018.
4) "Old Republic Title Announces Pavaso as National eClosing Technology Provider" Old Republic Title, 2018.
5) "The Importance of Educating Clients About the Threat of Wire Fraud" ALTA, 2017.
6) Standards for Safeguarding Customer Information, 16 CFR § 314 (2002).
7) Privacy of Consumer Financial Information, 15 CFR §313 (2000).
8) Protection of Nonpublic Personal Information, 15 U.S. Code § 6801 (1999).
9) 23 NYCRR 500.00 (2017).