Solving the Cybersecurity Riddle

A new cybersecurity solution designed for advisors keeps critical client data under wraps.

Today's cybersecurity challenges are unsolvable because cybersecurity products and services are based on a broken security model. Confidential consumer information is shared, sent, received, stored and accessed on or through the open internet which is fundamentally unsecured. It's like trying to protect swimmers in the ocean instead of a private pool

— Aaron Spradlin, chief information officer at United Planners

UNITED PLANNERS FINANCIAL SERVICES

For years, advisors have enjoyed the benefits of technological advancements. But along with the efficiencies these tools have offered, they've also led to an increasing array of digital threats for advisors and their clients. In recent years, major firms such as Equifax, Target and Uber have experienced high profile cyberattacks which exposed the personal information of hundreds of millions of consumers.

Both FINRA and the SEC have identified cybersecurity as a critical priority for financial advisors. Meanwhile, the risk has been elevated from stand-alone threats by individual hackers as evidence suggests that sophisticated and well-funded hacking teams are targeting firms in the financial services industry because of the breadth of personal and financial information held in these systems and databases.

In recent years, the challenge for advisors has been how to confront a problem that, in many ways, is outside of their control and simply can't be contained. Phishing attacks continue, ransomware attacks threaten advisors and their clients, and seemingly no network connection is safe from intrusion. As a result, advisors, their administrative support and their IT staffs are forced to play catch-up, constantly reacting to the next new threat through software patches and upgraded network components. The game of cat-and-mouse between hackers and their prey, however, continues as new methods are devised to infiltrate any given solution.

"Today's cybersecurity challenges are unsolvable because cybersecurity products and services are based on a broken security model," says Aaron Spradlin, Chief Information Officer at United Planners. "Confidential consumer information is shared, sent, received, stored and accessed on or through the open internet which is fundamentally unsecured. It's like trying to protect swimmers in the ocean instead of a private pool. Amidst this rapidly changing, fluid environment, today's secure solutions are tomorrow's compromised data breaches."

The good news is that there is a coordinated industry movement that is proactively taking on this critical challenge to avoid being reactionary. It is a consortium of financial industry professionals who are collaborating to improve end-to-end protection for financial advisors and their affiliated BDs and/or RIAs, as well as their peripheral circle of

It's cost prohibitive; it's complicated and it's not core to an advisor's expertise. The case for outsourcing comprehensive cybersecurity solutions is compelling

— Aaron Spradlin, chief information officer at United Planners

services providers such as custodians, money managers, financial planning providers and financial technology firms.

Addressing a Need

Advisors know that cybersecurity is critical. But when it comes to building a secure IT presence utilizing existing solutions and infrastructures, advisors have faced considerable roadblocks.

For starters, the costs can be prohibitive. Cobbling together a cybersecurity solution which includes an internal or outsourced Chief Information Security Officer (CISO) and network infrastructure to keep client data safe can cost tens of thousands of dollars. It also can be resource-intensive: The depth and complexity of cybersecurity threats, as well as the complexities of the systems designed to combat those threats, pose a tremendous challenge for advisors who attempt to manage these issues on their own. "It's cost prohibitive; it's complicated and it's not core to an advisor's expertise. The case for outsourcing comprehensive cybersecurity solutions is compelling," says Spradlin.

A reliance on routing traffic through the open internet requires ongoing vigilance to keep up with changing threats. Advisors and their information technology staff are constantly reacting to the latest malware, phishing and ransomware attacks. "Most cybersecurity efforts these days are focused on fixing broken things," says Sheila Cuffari-Agasi, Senior Vice President of Partner Development at United Planners. "That means trying to stay ahead of hackers by plugging gaps, employing encryption protocols, upgrading malware detection solutions, antivirus software, password managers and consistently training your staff not to click on 'anything suspicious,' which is an evolution in and of itself."

Choosing the right products or services from outside vendors also is challenging for advisors because of the lack of industry standards or regulatory framework around cybersecurity. The lack of an industry standard means advisors and their staffs must shoulder the burden of determining whether the products offer suitable protection and can be securely integrated with the rest of the system's components and platforms. Furthermore, there is always a concern of overlapping coverage and gaps across vendors.

Meanwhile, advisors must understand that failing to adequately protect critical client data can expose their firms to considerable jeopardy. For instance, the European Union's General Data Protection Regulation (GDPR) was put in force in May 2018 and is designed in part to levy considerable fines on companies which don't properly protect consumer data.

While GDPR only affects firms doing business in the EU, there is the potential that these types of regulatory protections will spread to other countries and regions. In fact, U.S.-based advisors already need to be following the Securities & Exchange Commission's regula-

Most cybersecurity efforts these days are focused on fixing broken things. That means trying to stay ahead of hackers by plugging gaps, employing encryption protocols, upgrading malware detection solutions, antivirus software, password managers and consistently training your staff not to click on 'anything suspicious,' which is an evolution in and of itself

— Sheila Cuffari-Agasi, senior vice president of United Planners Partner Development

tion and oversight of advisors, says Chris Arthur, Chief Compliance Officer of RDA Financial Network. "The SEC's rules are no joke," he says. "They want to know that RIAs are doing everything they can to keep the investor safe."

As a result, advisors would do well to stay ahead of that regulatory curve by adopting strict and up-to-date cybersecurity measures. What's more, failing to keep pace with technological advancements and digital security trends may leave advisors exposed. As trillions in wealth shift to younger generations in the next few decades, clients are likely to avoid advisors who prefer using a legal pad over an iPad. These advisors simply can't match the convenience and accessibility offered by more tech-savvy advisors, though the legal pad may offer better security if the iPad is not properly protected.

A Private Secure Network Solution

Broker-Dealers, RIAs, technology vendors and custodians are now working together within the consortium, founded by employees of United Planners Financial Services. Together, they are rallying to address the increasingly urgent cybersecurity needs of advisors. A key part of their effort focuses on the challenge of the open internet, where hackers and other bad actors acting with impunity, force companies to play catch up in a bid to protect their most critical data.

One approach, which has been implemented by United Planners as part of its cybersecurity offering, is to take confidential data off the open internet by utilizing a private secure network offered by cleverDome, Inc., an Arizona Benefit Corporation. The result: Traffic gets routed off of the open internet and into an invitation-only private network which requires authentication from every user and every device in order to access the information.

In a traditional network, data is routed through public internet servers. That data is vulnerable at many points in its journey from "Point A" to "Point B" because of the route it takes through these servers. Virtual Private Networks (VPNs) have offered a solution to this vulnerability, but at a cost to the user: Connections can be sluggish, adversely impacting productivity in exchange for security.

The cleverDome network, i.e. "the Dome," utilized by United Planners, and other BDs, RIAs, technology vendors and custodians, guards that data by routing it through a private network employing military-grade cybersecurity protection. This military-grade cybersecurity technology fractionalizes data, splits it up into many pieces and disperses the data over multiple channels. The result is a private network which is more secure, reliable and 10 times faster than a traditional VPN.

"The only real solution is to take confidential consumer information 'under the Dome™', which is secure and off the open internet," says Spradlin, who also helped build the cleverDome

UNITED PLANNERS FINANCIAL SERVICES

U.S.-based advisors already need to be following the Securities & Exchange Commission's regulation and oversight of advisors. The SEC's rules are no joke. They want to know that RIAs are doing everything they can to keep the investor safe

— Chris Arthur, Chief Compliance Officer of RDA Financial Network

network. "But to do that requires the creation of a global standard of trust, a trust network where participants know that other participants are secure under the Dome™."

Every member of the cleverDome network must meet certain standards and complete an in-depth due diligence process to gain access to the private network. That includes written assessments of cybersecurity controls, governance and compliance, and may even include site visits to confirm that necessary requirements for endpoint protection are met.

Beyond the Network

United Planners enhances its cybersecurity with additional security measures which extend through hardware, software and even human users.

Device Security: Only authenticated devices can access the Dome, limiting the number of potential threats. An app loaded on a computer, tablet or smartphone runs through a rigorous check of the device as it connects to the network, including the strength and age of passwords used, whether the device's critical software is up to date and how the device is connected to the network. (For instance, the app will reject a device if it's trying to connect via an unsecure public Wi-Fi network.)

If any of these criteria aren't met, the device is denied access to the Dome. The results of that authentication are relayed and monitored to a centralized dashboard that can alert end-users if there are authentication issues with a particular device. "It's an invitation-only network, and those that are invited must be authenticated," says Cuffari-Agasi. "It's the way to keep the system private and secure."

Training and Testing: Building a secure network and using the right hardware and software are crucial components of a strong cybersecurity plan. But just as important are how humans interact with those tools. Some two-thirds of cyber claims reported to insurers were due to human error such as employees being duped by phishing links or failing to take preventative measures such as regularly changing passwords[1]. United Planners' cybersecurity solution requires users to undergo training and testing to sharpen reactions to potentially dangerous situations such as phishing attacks. For instance, a user may receive a suspicious link intentionally sent by the United Planners' training system. If the user clicks on the link, the training system will inform that user of the failed test and the need to undergo additional training. The goal: reduce the instances of human error that can ratchet up cybersecurity risks for advisory firms.

One-on-One Support: As an extension of the United Planners Advisor Support Team, help is always available for issues that might come up for advisors utilizing this cybersecurity solution. Say an advisor loses her smartphone: The United Planners support team can

1 — Willis Towers Watson, "Decoding Cyber Risk: Driving a Cyber-Savvy Workforce," 2017.

Broker-Dealers, RIAs, technology vendors and custodians are now working together within the consortium, founded by employees of United Planners Financial Services

remove network authentication for that device to minimize the threat of a breach by an unknown user. Support can also help set up authentication for a replacement device and allow users access to non-confidential data while helping users remediate authentication issues. Due Diligence on Third-Party Vendors: Vetting the security capabilities of third-party vendors is a major stumbling block for advisors building their own system for cybersecurity protection. cleverDome, utilized by United Planners, addresses that issue by requiring compliance with minimum cybersecurity standards and completing due diligence on all firms that use the Dome, including software service vendors, portfolio accounting service providers, custodians and BDs. Any vendor who transmits, shares, syncs, or hosts client non-public information must pass the cleverDome due diligence process. "This is a solution that works for the industry, the advisors and the vendors," says Spradlin. "It was a problem that needed to be solved, and solved in the right way."

A Turnkey Solution

In the search for cybersecurity solutions, advisors have largely been left to build systems on their own. That may be why just 4.1 percent of financial institutions plan on adopting new cybersecurity measures this year, and why nearly 75 percent of institutions are still using systems that are five or more years old[1]. The challenge of choosing each component of their system, from antivirus protection and firewalls to help-desk support and email monitoring, can be dizzying even for the most tech-savvy advisor.

United Planners relieve advisors of those burdens with a robust, holistic cybersecurity solution that delivers a full suite of security and administrative offerings, including antivirus and malware protection, encryption, cyber insurance, training and customized support.

"The goal is to protect advisors," says Cuffari-Agasi. "We want advisors and their clients to be protected without them having to become experts in this arena, or having to educate themselves about how to do vendor due diligence. Technology is an increasingly important part of the advisory industry, and advisors need to be able to take full advantage of these tools without putting themselves or their clients at risk."

Next StepsPlanning

There's no one-size-fits-all cybersecurity solution for financial advisors. Each firm has different needs and faces different threats. However, there is common ground: All advisors need to take a proactive approach to protecting their client's data, and build plans for their firms that recognize the constantly shifting nature of the technology environment. If they don't, advisors face a range of threats, from steep regulatory penalties to the catastrophic reputational risks that can accompany these types of issues.

Fortunately, advisors don't need to do this work alone. For instance, United Planners offers advisors information on

1 — DALBAR, "State of Authentication in Financial Services," 2018.

UNITED PLANNERS FINANCIAL SERVICES

The only real solution is to take confidential consumer information 'under the Dome™', which is secure and off the open internet. But to do that requires the creation of a global standard of trust, a trust network where participants know that other participants are secure under the Dome™

— Aaron Spradlin, chief information officer at United Planners

these issues in a dedicated Cybersecurity Resource Center on its advisor website platform called connectUP. United Planners also offers one-on-one guidance to help advisors build cybersecurity plans that fit their needs and address the unique security challenges that they face. "The good news is that there are a lot of people out there working on solving the cybersecurity problem," says Spradlin. "In the meantime, advisors need to take smart steps to give their clients and their firms the best protection they can. After all, this is no longer a threat that advisors can afford to ignore."

Case study: Chris Arthur and RDA Financial Network

A few years ago, Chris Arthur saw that cybersecurity was become a larger, more menacing threat to the financial advisory industry. Arthur, Chief Compliance Officer with RDA Financial Network in Coralville, Iowa, decided to take action.

He started by asking colleagues and industry contacts how other firms were handling cybersecurity. What he found was that many companies were taking a shotgun approach to cybersecurity. Arthur viewed a company's SEC-mandated cybersecurity plan and was surprised by how it scarcely addressed the real issues of cybersecurity. "It was paralyzing," he says. "It was slapped together and nothing was organized. I couldn't understand how, with 60 pages of information, just a fraction of it tied into cybersecurity issues."

Arthur also viewed the SEC's cybersecurity audit questionnaire, which was more than 70 detailed questions about how firms were prepared to handle a range of potential scenarios. The SEC's questionnaire made Arthur realize just how inadequate much of the advisory industry's response to cybersecurity has been.

Arthur immediately went to his firm's IT professionals to ask for help in building a cybersecurity plan. It soon became clear to Arthur that the IT professionals were in over their heads. He finally told Arthur that he wasn't equipped to handle such a massive project, and that doing so would require considerable resources and a five-figure bill for the RDA Financial Network.

Arthur regrouped and came up with a plan: He'd handle writing the documentation his firm needed, such as cybersecurity policies and procedures for employees; business continuity and disaster and recovery plans; an advisor termination checklist that would quickly remove a former employee's credentials to access the firm's data. Next, he called United Planners to address a range of critical cybersecurity issues such as vendor management.

The move to address his firm's cybersecurity issues was no picnic. But in his detailed search for answers, Chris Arthur is confident that the solution used by his firm gives them the best preparation against ever-present cyber threats. "What United Planners offers is a plug-and-play, turnkey solution for cybersecurity," he says. "And for firms in this industry, that is a real relief.".

UNITED PLANNERS FINANCIAL SERVICES

The United Planners approach to cybersecurity

A holistic approach to cybersecurity includes technology as well as administrative components. Here are some of the key attributes of United Planners' cybersecurity solution:

- Firewall
- Encryption
- Antivirus (malware/spyware)
- Password Manager
- Email Monitoring/Storage/Hosting
- Cybersecurity Insurance
- Regulatory/Compliance Audits
- Help Desk Support
- Vendor Due Diligence
- Endpoint Protection
- Training and Testing
- Transmission of Data Through a Private Network

To learn more about how United Planners' unified approach to standardized security can be of value to you and your clients, contact Partner Development at

800-966-8737

United Planners Financial Services
7333 E. Doubletree Ranch Road, Suite 120
Scottsdale, AZ 85258

www.UnitedPlanners.com

UNITED PLANNERS FINANCIAL SERVICES