National Cyber Security Awareness Article Series

Key actionable insights for registered investment advisors

ABOUT ALIGN

Align is a premier global provider of technology infrastructure solutions and cybersecurity services. For over 30 years, the world's leading firms have relied on Align to guide them through IT challenges, delivering complete, secure solutions for business change and growth. The company's products and services include Data Center Solutions, IT Advisory Services, Cloud Services, Cybersecurity Risk Management, Technology Relocations, Workplace Technology, Outsourced IT Support, Project and Technology Management, IT Managed Services and Professional Services.

Align is headquartered in New York City and has offices in London, Chicago, San Francisco, Arizona, New Jersey, Texas and Virginia. Learn more at: www.align.com and www.aligncybersecurity.com

TABLE OF CONTENTS

INTRODUCTION

The cybercrime ecosystem continues to burgeon and evolve, given new innovations, the rise of sophisticated onslaughts and the internet of things (IoT). To assist firms in staying abreast of cybersecurity best practices and hot topics, Align is excited to share our National Cyber Security Awareness Month (NCSAM) Article Series.

The series covers an array of topics related to cybersecurity risk management, including common misconceptions, mobile security, phishing, cyber insurance, securing cloud IaaS resources and 2018 trends. Contributors to the NCSAM Series include executive leadership at Align, Iron Cove Partners and RootSecure.

Our mission is to empower you with expert insight, so you can enhance your security measures and make the most of today's technology and resources.

THE TOP THREE COMMON CYBERSECURITY MISCONCEPTIONS

BY: ALIGN

Cybersecurity has become a primary concern worldwide, even more so in the past few weeks since the exposure of personal information of 143 million Americans. How can we more effectively protect ourselves from cyber threats? A starting point is debunking the most common misconceptions held by far too many end users.

Myth #1 – My company isn't a large enterprise; I'm not a target to cyber criminals.

Many small businesses have their guard down because they do not consider themselves to be an attractive target to hackers. The truth is, most businesses that have suffered some type of data breach in 2017 have under 1,000 employees. Hackers are in fact hedging their bets on this misconception held by small businesses because they are looking for a fast, easy target. Hackers realize that small business have likely invested less in cybersecurity, because they believe that their data is not at risk. To undermine the efforts of hackers, understand that anyone and everyone is a target of cyber-attacks. The question is not when in the future will you be hacked, but has it already happened and you don't realize it? Get ahead of hackers and consider cyber defense strategies.

Myth #2 – I cannot prioritize cybersecurity because I cannot afford it.

If you believe that Myth #1 is true, you may inevitably believe Myth #2. The truth is, it may be impractical for your business to invest in cybersecurity now, if the budget is tight, but if you are hit with a cyber-attack, you may ultimately never recover from the costs of a breach. The costs will not only include the insurmountable legal fees incurred, but the immense damage done to your reputation. Even if your business does eventually recover monetarily, your end users may choose to never trust you again to responsibly protect their data. Invest in cybersecurity now, so you can avoid spending on the fallout of a breach.

Myth #3 – Technology will deal with it.

The easiest component of businesses for hackers to target: unsuspecting, unwary employees. They have become the weakest link in the chain, possibly because their employers believe Myth #2. Countless data breaches have originated from a single phishing email. Chances are, the employee who opened the phishing

Myth #1:

My company isn't a large enterprise; I'm not a target to cyber criminals.

Myth #2:

I cannot prioritize cybersecurity because I cannot afford it.

Myth #3:

Technology will deal with it.

email, and exposed the entire company to attack, simply was not trained to be suspicious of such an email. While it is easy to paint one individual as ignorant, the problem lies in the bigger picture: their company did not provide adequate training. It is crucial to focus on educating employees, so that attack prevention can begin with them.

Today, it is abundantly clear that **no one is immune to cyber-attacks**. Business after subsequent business have found themselves the target of hackers, and much of the time it is long after the data has been compromised. This is demonstrative of the criticality and expectation that businesses invest in employee education and cybersecurity technologies to curb and mitigate cyber-attacks. The consequences of a security incident, ultimately outweigh the investment that it requires of a firm. Defend your data and that of your customers, before it becomes too late.

HOW TO PROTECT YOUR FIRM IN A BYOD WORLD

BY: ALIGN

How often do firm employees complete work tasks on a personal phone or laptop? The answer might be every day. This is commonly known as BYOD, or Bring Your Own Device. Firms that allow employees to use personal devices for business purposes, need to clearly define policies and procedures to reduce security risks. Maintaining work data on a personal device creates an opportunity for risk and therefore, requires a great deal of device vigilance and proactive security measures.

If a device is lost or stolen, sensitive business information can fall into the wrong hands, compromising company data. The following are some tips for strengthening your firm's mobile security.

Authentication

Accessing company data on a personal device is made far more secure by enabling two-factor authentication. This requires a user to authenticate using two components before they can utilize a service. An example of this is when a user logs into a web application with a username and password (or passcode) and following the password submission, the user is then required to enter a verification code to proceed with authentication. This code is delivered via text to another trusted device in the user's possession, or by email. The verification code expires after a short period of time to prevent reuse. Additionally, the use of biometric technology, such as Windows Hello facial and fingerprint recognition, can be used for two-factor authentication. If your device is stolen, accessing its content without authenticating will be extremely difficult.

Encryption

In the event that an employee or contractor loses their device, firms should proactively utilize storage encryption technology to mitigate risk. Windows' BitLocker Drive Encryption is a data protection feature that is designed to protect user data and prevent tampering. BitLocker provides full disk encryption and aims to prevent unauthorized access, by enhancing system protection, and will render data inaccessible from decommissioned computers. The only way to decrypt the disk is with a key that is sent to a Microsoft or Active Directory account that is associated with the device. Additionally, BitLocker can be configured to lock during the startup process until a user provides a PIN or a removable device, such as a USB drive, containing a startup key. Both of which are further examples of multifactor authentication. The machine will not be able to resume from hibernation mode until the required authentication tool is supplied by the device owner.

As you develop your company's BYOD strategy, be sure to consider the following aspects:

- Mobile Device Management (MDM) Policy
- Acceptable Use Policy
- Supported Devices
- Disclaimers/Risks/ Liabilities
- Password Policy
- User Acknowledge-ment and Agreement

Taking these steps will help to secure and control sensitive corporate data on BYOD devices.

Remote Control

Firms can install software on personal devices so that, if they are stolen or misplaced, the contents can be wiped remotely. Businesses can also be selective in what data is erased. For example, they may remove corporate data but allow the personal data to remain. The device can also be remotely locked and a password reset can be performed if necessary. An example of this software is Windows Enterprise Mobility and Security Suite's Selective Wipe tool.

Secure Connections

While protecting your device is crucial, it is also imperative that you be aware of your surroundings while using your device to access company resources. As a best practice, you should avoid completing work duties over an unsecured wireless channel. Instead, utilize a Virtual Private Network (VPN), which will encrypt data transmission between your location and work, making it illegible to outside parties. This can be easily enabled on smartphones and laptops. Essentially, it creates an encrypted tunnel that only authorized users can access and data cannot be intercepted. The VPN is likely behind a firewall, making interception even more difficult.

Policies and Procedures

It's crucial for firms to implement a thorough BYOD policy to maintain the confidentiality of data and help protect the company from security threats. Security controls, such as mobile device management (MDM), act as an extension to the organization's overall breach prevention strategy. This enables enterprises to centrally manage policies, apply them from the cloud and protect business data on mobile devices. Not only should the policy be enforced, but firms should also provide employee security awareness training. Training modules will help staff to understand BYOD policies and guidelines, as well as, the risks associated with BYOD devices.

CYBERSECURITY COMPLIANCE

By: John Araneo, General Counsel and Managing Director, Align

Background

The Cybersecurity phenomenon has changed the risk management game categorically. The world's largest and most prominent corporations have fallen victim to both sophisticated and rudimentary attacks. Prominent law firms, big banks and world-class accountancy and consulting firms have all been successfully attacked. Government entities (even those that regulate and enforce cybersecurity compliance), elections, buildings, utilities, devices and, well, the list of targets goes on and on. Cyber-attacks are as invisible as they are pervasive, as ephemeral as they are indelible. Indeed, recent events clearly demonstrate that cyber threats have created a new risk management paradigm entirely. In determining how to approach cybersecurity compliance, there are several threshold issues that every organization must consider.

A Dynamic, Multi-factorial Issue

Cybersecurity compliance presents a dynamic, multidisciplinary challenge that requires a collective effort between typically dislocated business units and personnel with disparate skill sets. There are several factors involved – the IT architecture, technologies, employee awareness, various workflows and data usage practices, third-party management and ever-evolving threat points and attack vectors. Making matters worse, the legal landscape is a patchwork of federal statutes, state laws, regulations, industry-specific rules and emerging best practices. Although this body of jurisprudence is far from being harmonized, there are certain core elements that are taking form as reliable "common denominators" for cybersecurity compliance. We have found that under all the governing laws and pertinent rules and regulations, creating a model Cybersecurity Program time and time again requires input from various sources, including:

- Legal/compliance, to understand legal/regulatory landscape;
- IT, to understand the current IT architecture and its limitations;
- HR, to address employee training needs;
- Operations, to understand the firm's data work-flows;
- Third parties, to understand and address vendor risk; and
- Management to identify all IP and data inventory, to understand the types of data the firm stores, transmits or uses, such as confidential, third party, proprietary, or other sensitive data.

And even then, each firm needs to weave these data points together and design a thoughtful, compliant and highly tailored Cybersecurity Program that creates a viable framework for addressing the attendant risks involving its customers, vendors, employees and its counterparties. Clearly, a multi-disciplinary approach is critical to building an unimpeachable, model Cybersecurity Program.

A Culture of Compliance

The installation of a point-person or a manager of the program, a Cybersecurity Program Administrator, is a good first step and in fact, under most regulatory regimes, it's generally required. But the organization's commitment to cybersecurity compliance must be deeper than that. The Cybersecurity Program Administrator must be empowered to effect change and be held accountable if the program fails. Straddled between the administrator, company leadership above must demonstrate a full-throated buy-in, to putting cybersecurity as a top-line focal point and the employees below must be compelled, encouraged and/or incentivized to increase their knowledge, awareness and proficiency of these risks and how the program attempts to address them. Once the program has been successfully imbued throughout the organization, an external exercise should ensue, wherein the organization must ensure the same or similar controls to that of its program have been adopted by certain of its vendors, counterparties and other third parties.

The Human Element

Ironically, this inherently digital phenomenon invariably breaks down due to human error and/or manipulation. No technology, no black box and no IT architecture can remove this variable from the cybersecurity risk matrix. An organization's staff – its employees, consultants, advisers and other agents -- serve as its human firewall. Just as firewalls need to be updated and enhanced to maintain its capabilities, employees and staff members also need to be updated and trained on the basic concepts of security awareness as well as with regard to emerging threats and risks. All employees should receive routine training and be subject to testing and phishing campaigns. Moreover, the education program should be reportable and trackable, to ensure each employee receives additional training when necessary.

Putting the Pieces Together

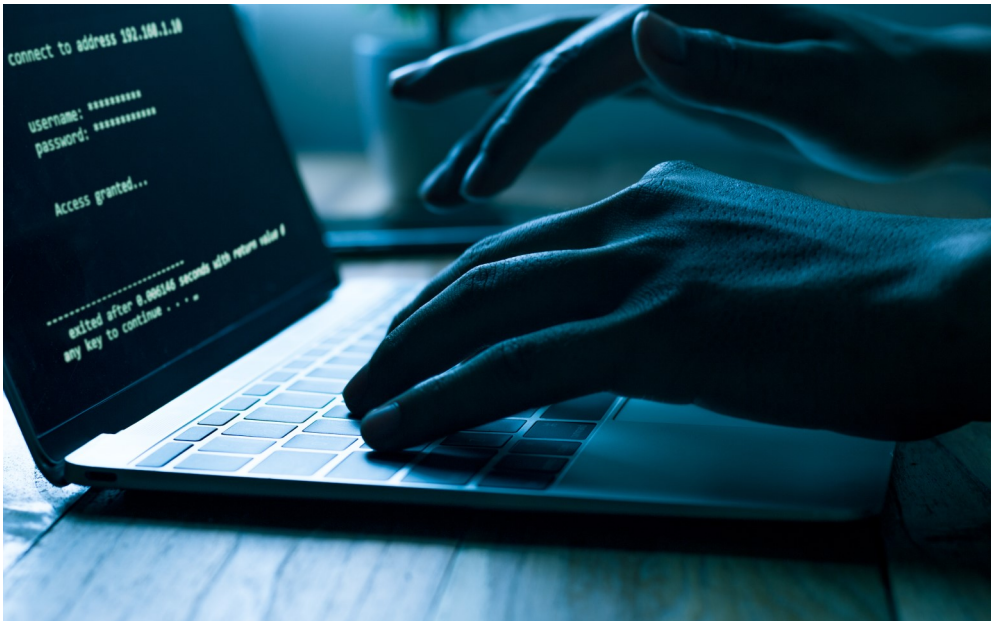
Building a model Cybersecurity Program is generally perceived to be somewhat of a harrowing, anomalous exercise because it involves creating a synergy between typically dislocated workflows and unfamiliar technical experts in one underlying framework. And there really is no way around this and, in fact, the global cybersecurity spend has been reported to exceed $86.4 billion, this year alone. The reality is that, like many compliance endeavors, those that approach cybersecurity compliance methodically (as a journey, not a destination) and routinely (think quarterly and annual assessments), will show that it's not impossible to 'crack the code' of cybersecurity compliance.

"It's not impossible to 'crack the code' of cybersecurity compliance."

About the Author

John Araneo, Managing Director and General Counsel of Align Cybersecurity

John remains a practicing attorney with Cole-Frieman & Mallon, LLP, a firm that represents over 600 asset management clients and launches approximately 70 private investment funds annually. Having followed the regulatory initiative on cybersecurity in the alternative asset management space since its inception, John is an established author, cybersecurity expert and well-known thought leader on the legal, regulatory and governance issues related to cybersecurity.



WHY SHOULD REGISTERED INVESTMENT ADVISORS BUY CYBER COVERAGE?

BY: LOUIS D'AGOSTINO, IRON COVE PARTNERS

Cyber breaches. Rarely does a day go by without breaking news on yet another high-profile attack. Equifax. Yahoo. Target. Home Depot. Ashley Madison. Even the governing body of the financial services sector, the powerful Securities and Exchange Commission, announced their EDGAR Database was compromised in late 2016. The more notable the target, the bigger the headline. But, it isn't only multinational corporations and government entities which are breached.

Cyber risks are ever-present for businesses of all sizes, and Registered Investment Advisers and Investment Managers are no exception. Along with an increasing frequency of attacks, the cost and severity of attacks continue to rise, as well. The need for a robust cyber insurance program has never been greater.

Over the last several years, C-Suite executives at investment advisory firms began to monitor and track the evolution of cyber risks, particularly as it related to the increasing complexity of data and privacy security issues for their firms. This has led to the internal development of policies and procedures, as well as incident response plans, to prepare for and prevent such an attack. Simultaneously, we have seen a significant uptick in resources assigned to intrusion detection and penetration testing. Without question, these are signs that firms are beginning to take a proactive approach to cybersecurity.

The last SEC alert, from the Office of Compliance and Inspections and Examinations, concluded that advisories have dedicated more resources to guard against these potential risks, citing an increased level of preparedness since its last initiative, back in 2014. Of course, cybersecurity remains a priority for SEC regulators, as well as other Self-Regulatory Organizations.

What are the Risks?

Incident response plans are designed for occasions when personally identifiable information (PII), non-public private information (NPPI), confidential employee records, trade secrets, or intellectual property are divulged. A breach which would make this information vulnerable may occur by way of malware; social engineering attacks; lost or stolen devices, such as laptops and storage devices; malicious insiders; or unintended disclosure.

"Cyber risks are ever-present for businesses of all sizes, and Registered Investment Advisers and Investment Managers are no exception."

Pointedly, malware attacks, which infect networks and shut-down computer systems, can be a major disruption to an investment advisory's business.

Internal Costs to a Firm

- Detection
- Investigation to uncover the scope and nature of the breach
- Containment and preservation of existing systems and data
- Recovery
- Ex-post response

External Costs to the Firm

- Loss or theft of information
- Business disruption
- Damage to equipment
- Loss of revenue and additional expenses
- Loss of Customer Assets

With such high costs associated with a breach, it is clear that insurance should be a part of every advisory's cybersecurity program. And, yet, only 35% of advisors carry such coverage.

Why Should Advisors Carry Insurance?

In the event of a data security and privacy breach, the costs associated with putting an incident response plan into action are high. According to the Ponemon Institute's *Cost of Cyber Crime Study*, the median annualized cost of a 2016 cybercrime is $6.7MM, up from $5.5MM only a year earlier.

Ultimately, this is a cost which, with an appropriate internal risk assessment, could have been wholly transferred to an insurer.

Regulatory Guidance and Operational Best Practices

When regulators make "suggestions" and provide "guidance," as to what a robust cybersecurity program should look like, it would be foolish not to take heed. Since 2015, RIAs have consistently been put on notice that the SEC considers cyber insurance to be part of a balanced, robust security program. At the same time, all industry regulators have made cybersecurity a top priority, dedicating significant resources to the cause.

The implementation of these best practices demonstrates that firms take these risks seriously, instituting a culture of compliance and consumer protection. However, for those firms which take business continuity seriously, there is no substitute for cyber insurance.

Investor Due Diligence

Operational due diligence, conducted by larger institutional investors when determining which RIAs are suitable investment risks, most certainly requires that firms have adequate policies and procedures in place to deal with the potential of a cyber incident, in addition to adequate coverage to manage the aftermath of such an attack.

Cyber Coverage Still Underpriced, Set to Increase – Act Now to Lock in Lower Rates

With premiums in the range of $2,500 to $4,500 per million dollars of coverage, rates remain at historic lows due to an influx of new carriers and increased capacity. For now, cyber coverage remains cost-effective and economically feasible. However, as the number of claims increase, the costs associated with this type of coverage will increase, as well. Now is the time for RIA executives to take advantage of competitive premium rates in a very soft insurance market.

About the Author

Louis D'Agostino, President & Financial Services Practice Leader of Iron Cove Partners, LLC

Louis is a dynamic senior insurance professional with nearly 17 years of experience in the financial services industry. He is presently serving as the President and Financial Services Practice Leader of Iron Cove Partners, LLC. He is dedicated to business and product development and large account placement, resulting in a proven track record of successful negotiation of even the most challenging of claims such as Madoff, investor litigation, and SEC/DOJ enforcement. As part of his work at Iron Cove Partners, Mr. D'Agostino's expertise has been called upon by a variety of industry trade groups. Prior to accepting his role with Iron Cove Partners, LLC, Mr. D'Agostino spent 10 years working for Frank Crystal & Co., a NYC-based insurance agency founded in 1933. His final role with the organization was as a Director in the Financial Services Department where he was able to perfect his negotiation skills. He successfully placed Management and Professional Liability Insurance on behalf of numerous financial institutions including hedge and private equity funds, registered investment advisors, securities dealers, and consultants. With a diverse battery of skills and experience, Mr. D'Agostino has managed accounts for commercial businesses including real estate, not-for-profits, manufacturing, retail, and tech firms.

Phishing Statistics 2017

- The most popular email phishing lures are **fake invoices.**
- **Apple IDs** are the #1 target for credential theft emails.
- Phishing volume peaked in the middle of the year during **major global events**, such as Brexit.
- Email remains the #1 attack vector for most malware.
- Over 400 businesses are targeted by **Business Email Compromise (BEC)** attacks, or CEO Fraud, daily.

SOMETHING SEEMS "PHISHY" – HOW TO IDENTIFY AND AVOID PHISHING SCAMS

BY: ALIGN

Phishing is a popular scam tactic that attempts to fool its victims into giving out personally identifiable or company information. Many phishing attacks are driven by monetary gain, but in other cases they simply aim to wreak havoc on a specific company or even an entire country. Phishing attacks often take the form of fraudulent emails, some of which contain malware or ransomware that propagates when a user opens or clicks on the email contents. Phishing often relies on the use of **social engineering** techniques. Social engineering is a psychological tool that takes advantage of patterns of human behavior. One of these patterns being that people are inclined to blindly open email, especially if they are motivated by curiosity, fear, urgency or opportunity. Perhaps an email contains an urgent or intriguing subject line, or contains a document attachment that appears to be work related. Below we will explore some of the most common phishing email attacks seen in 2017.

Business Email Compromise (BEC)

One type of email phishing attack is the **Business Email Compromise**. Business Email Compromise, or BEC, attacks take a few different forms. The first is **CEO fraud**, in which a CEO's email address has been successfully spoofed. Spoofing may require the attacker to create an email address that appears to have originated from the CEO, or the attacker has been successful at compromising the CEO's inbox and is able to send out emails from the legitimate email address. Using the spoofed email address, the attacker will request an urgent wire transfer from another, likely less senior, employee. The less senior employee may be susceptible to the social engineering tactic which emphasizes the urgency and seniority of the request. In addition to the theft, the attacker may also inject malware into the company to gain further infrastructure access.

The second form of BEC are **bogus invoice scams**, in which the attacker again spoof's the executive's email account or gains access to their mailbox. The attacker locates a bill that is due soon in the executive's inbox. The attacker then

contacts the accounting department to change the payment location to an account that the attacker owns. **Attorney impersonation** is another common form of BEC attacks. If an attacker is able to successfully impersonate a company's law firm they may request funds to settle a legal dispute or pay an overdue bill. The FBI has reported that the BEC scams cost businesses **$3.1 billion**. These attacks have increased by **1,300%** since January 2015.

Ransomware

Ransomware is often delivered to phishing victims via fake email invoices. Attackers may schedule the phishing invoices to be sent specifically during work hours, to both make the emails appear to be legitimate, and to catch victims when they are somewhat distracted; another example of a social engineering tactic. Once the victim opens the email, they will see it contains an attached zip file, presumably containing the invoice, that once clicked on, executes the attacker's ransomware.

Ransomware targets and encrypts specific file extensions on a system, which in many cases will render the machine utterly useless. The files will remain encrypted until the ransom is paid to the attacker. Unfortunately, often times a ransom is paid by the victim and the files are not decrypted. Millions of users have been subject to this attack and have paid millions of dollars in ransoms. Ransomware is very effective and lucrative for attackers, and the number of victims will only continue to rise.

Google Docs

The Google Docs phishing scam has affected over three million people worldwide. While this scam has been in existence since 2014, the latest attack is particularly effective, in part because it looks very authentic. The attacker sends a fraudulent invitation to edit a Google document to the victim. After clicking the document link, the victim is led to a genuine account screen, which shows all of the Google accounts that they are presently logged into. The authentic screen only entices the victim to move further into this scam. After choosing the account to log in with, a malicious third-party app, masquerading as Google Docs, asks to be granted privileges to access account information. Granting this permission provides all of the victim's account information to the attacker. This scam is particularly effective, not only because it mimics Google so successfully, but because the attacker can continue stealing information for as long as the victim is unaware that their account has been compromised.

How to Avoid Being Phished

Being that phishing email tactics have become increasingly sophisticated and convincing, it is important to be on the lookout for the following:

- **Scrutinize the domain name of the sender**. At first glance @gmail.com may look similar to @gmai1.com. Attackers often take advantage of similar looking characters in order to spoof email addresses.
- **Rather than clicking on embedded links in an email, hover over them.** If the link address looks to be unusual, best not to click on it.
- **Look for spelling mistakes.** Authentic emails from well-known brands typically do not contain spelling or grammatical errors.
- **Companies with which you have an account typically use your name.** They will generally not address you as a generic "Valued Customer".
- **Banks and other companies never ask for personal information.** Do not ever give out personal information or user credentials.
- **Don't be fooled by urgent language in the subject line.** Remember that attackers are hoping to instill panic in victims when they read "Unauthorized login attempt".
- **Check email signatures.** Legitimate senders almost always provide contact details.
- **Do not open attachments from unfamiliar senders.**

As demonstrated by some of the most wide spread and devastating phishing attacks, no one is immune to falling for a phishing scam. Educate your firm with employee security awareness training. Phishing training modules will allow your employees to become experts at identifying phishing emails; before they fall victim to phishing attacks in the wild.

SECURING AZURE IAAS RESOURCES

BY: CHRIS MIHM, DIRECTOR OF MANAGED CLOUD SERVICES AT ALIGN

Microsoft Azure makes it simple to deploy IaaS resources in the public cloud. As a result, it can become easy to forget, or even bypass, best practices for securing your Azure IaaS resources. The following is a list of common best practices that may be utilized when deploying Azure resources via the Azure Resource Manager (ARM) portal. Specific use cases will ultimately dictate deviation when necessary, but for most deployments, these hold up.

Virtual Private Network

Creating a Site-to-Site (S2S) VPN connection between your on-premises network and your Virtual Private Network in Azure provides a secure, dedicated, IPsec tunnel for communicating. With a Site-to-Site VPN connection in place, you can completely remove specified public access and simply connect via the internal ports as you would with any other machine on your internal network. Another option is to create a Point-to-Site (P2S) VPN connection, which establishes a secure connection directly from a computer to the Virtual Network without having to acquire and configure a VPN device, as would be necessary for a Site-to-Site VPN connection. Both S2S and P2s are great ways to reduce external threats by removing the public facing access. See Create a Site-to-Site connection in the Azure portal for setting up and configuring a S2P VPN connection. Additionally, see Configure a Point-to-Site connection to configure a P2S VPN connection.

ExpressRoute

ExpressRoute creates private connections between Azure datacenters and either on premises infrastructure or in a co-location environment. ExpressRoute connections are not transmitted over the public Internet, and offer greater reliability, faster speeds, lower latencies and higher security than typical connections over the Internet. With ExpressRoute, you can establish connections to Azure at an ExpressRoute location or directly connect to Azure from your existing WAN network provided by a network service provider.

Secure Endpoints with Network Security Groups (NSGs)

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets and individual network interfaces attached to VMs (Resource Manager). When you deploy a virtual machine, a default NSG is created with 1 inbound security rule to allow VM management. The VM is initially be configured with a public IP. It is recommended to dissociate the public IP from the Azure Arm portal in order to remove public facing access to the VM. This is a great way to reduce external threats.

Usernames, Passwords and Multi-factor Authentication

When provisioning and accessing resources in Azure, users are required to authenticate. Enforce complex usernames and passwords for your VMs. Azure requires passwords to be between 12 and 123 characters long and must contain 3 of the following: a lowercase character, an uppercase character, a number and a special character.

In addition to strong passwords, it is good practice to enforce multi-factor authentication which adds a second layer of security to user sign-ins. This reduces the likelihood that compromised credentials will have access to an organization's data.

Manage your VM security posture with Azure Security Center

Azure Security Center provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. It delivers visibility and control over hybrid cloud workloads, active defenses that reduce your exposure to threats, and intelligent detection to help you keep pace with rapidly evolving cyberattacks with active threat monitoring and security alters.

Security Center is offered in two tiers:

- The **Free** tier is automatically enabled on all Azure subscriptions, and provides security policies, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.
- The **Standard** tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier provides advanced threat detection capabilities.

For more information on Azure Security center, see Introduction to Azure Security Center.

Protect data at rest in VMs by enforcing encryption

For many organizations, data encryption at rest is a mandatory step towards data privacy, compliance and data sovereignty. Azure Disk Encryption enables IT administrators to encrypt Windows and Linux IaaS Virtual Machine disks. Azure Disk Encryption protects and safeguards data to meet organizational security and compliance requirements. Encryption mitigates risks related to unauthorized data access. Organizations that do not enforce data encryption are more likely to be

"Microsoft Azure makes it simple to deploy IaaS resources in the public cloud. As a result, it can become easy to forget, or even bypass, best practices for securing your Azure IaaS resources."

exposed to data integrity issues, such as malicious or rogue users stealing data and compromised accounts gaining unauthorized access to unencrypted data.

For more info visit, Azure Data Security and Encryption Best Practices.

In addition to the above recommendations, there are other numerous methods that are available to secure Azure IaaS resources. Documentation on these resources can which can be found at Microsoft. Further information regarding Align's cloud services offerings can be found here.

About the Author, Chris Mihm

Chris Mihm, Director of Managed Cloud Services of Align

Chris is the Director of Managed Cloud Services at Align. He is an IT professional with over 19 years of experience in customer facing roles including designing, architecting and managing the implementation of cloud solutions, information systems and technologies for small to mid-size companies. He has a broad range of skills and knowledge around virtualization and cloud technologies.

5 KEY COVERAGE ELEMENTS OF A COMPREHENSIVE CYBER INSURANCE PROGRAM FOR REGISTERED INVESTMENT ADVISERS

BY: LOUIS D'AGOSTINO, IRON COVE PARTNERS

For investment advisory firms purchasing insurance to protect against a cyber incident, it is important to note that not all policies are created equal. Many such policies were written to address cyber risk for general commercial businesses, and not necessarily with financial services firms or their unique risk profile, in mind.

The business profile of a registered investment adviser is different than that of your standard small business, as managing high net worth or institutional assets introduce a unique set of risks, especially as it relates to cyber and data security.

RIAs amass confidential, personally identifiable information, as well as non-public private information, from their clients. Additionally, access to computer systems and telephony is a critical part of business infrastructure. Denied access to networks or telephone systems would cause a major disruption to any small, service-based business, let alone an RIA.

Other concerns specific to RIA cyber risk, include fines and penalties, loss of fee-based revenue, regulatory defense costs, and, perhaps most importantly, the loss of customer capital as a result of a social engineering scam. This means that reviewing insuring agreements and policy provisions is more important than ever.

Understand Your 3rd Party Liability Coverage

3rd Party Liability Coverage provides protection for an adviser for liability resulting from a data/privacy security incident. The most important types of 3rd Party Liability Coverage are Privacy, Network Security & Media Liability.

- **Privacy Breach**: Liability arising out of the disclosure of personally identifiable information and, in some cases, non-public private and confidential information.
- **Network Security Incident**: Liability arising out of unauthorized access, a denial of service attack, or the downloading of malicious code.

- **Media Liability**: Liability which arises from defamation, slander, libel, and copyright infringement.

Additionally, while most policies' coverage includes regulatory defense expenses, fines and penalties are only covered under select policies. Broader policies will include coverage for regulatory fines and penalties; however, the insurability of fines and penalties by regulators is contingent on state domicile and whether coverage is allowed by state law. In any case, such coverage is an important component of any comprehensive cyber insurance strategy.

What 1st Party Coverage Does My Policy Include?

1st Party Coverage is made up of the elements of protection which would provide an insured adviser with coverage for direct costs resulting from a cyber incident.

1st Party Coverage Would Include:

- Business Income and Extra Expense coverage
- Public Relations and Crisis Management costs
- Notification Expenses
- Forensic costs to investigate a cyber event
- Software and Electronic Data Restoration
- E-Extortion Expenses
- Cyber Crime and Social Engineering

While some 1st and 3rd party insuring agreements are automatically included as part of "cyber package" policies, some offerings may not fully relate to the needs of an RIA and, as such, should be removed. For example, why would an RIA need coverage for PCI Fines and Penalties when they don't accept credit cards? And, why have coverage for Business Income Loss if an RIA couldn't possibly prove a loss of business income (e.g. advisory fees on managed assets) due to a cyber breach? Moreover, many policies specifically state that business income shall not include "fees," which, in most cases, would preclude an adviser from collecting on any loss of income.

5 Things Every Investment Adviser Should Consider:

1. Evaluate your Business Income Coverage: You may be paying for coverage which will never apply. Alternately, the calculation methodology may not meet your business needs.
2. Beware of Problematic Exclusions: Make sure your policy doesn't exclude acts of foreign enemies. We believe that any unauthorized access or cyberbreach could be construed as an act of a foreign enemy, leaving you without coverage.

1st Party Cyber Coverage Includes:

- Business Income and Extra Expense coverage
- Public Relations and Crisis Management costs
- Notification Expenses
- Forensic costs to investigate a cyber event
- Software and Electronic Data Restoration
- E-Extortion Expenses
- Cyber Crime and Social Engineering

3. **Remove any exclusion related to failure to patch software (e.g. Petya Virus):** This type of exclusion is clearly problematic given that the recent Petya ransomware attack can be traced back to a vulnerability in Microsoft software. If an insured adviser was impacted by such a ransomware attack, no coverage would have been available.
4. Make sure your incident response team and related vendors are approved by your insurance carrier in advance of any incident, as it is required by some carriers.
5. Coverage for Social Engineering Crimes and loss of customer capital may have to be added to your policy or at a minimum, you may need to secure this coverage separately.
6. Be sure consultants, vendors, and independent contractors are covered by your policy. There are numerous instances where consultants, vendors and independent contractors have access to RIA systems and networks. Vicarious Liability for such individuals must be contemplated as part of a robust cyber insurance program!

VULNERABILITY MANAGEMENT – THE KEY TO CYBERSECURITY SUCCESS

BY: SETH ARBITAL, CHIEF INFORMATION SECURITY OFFICER OF ALIGN

"The key is for the gentleman, the crook finds a way." While this is true, we still place strong locks on our doors and valuables, and set alarms. Threat actors are continuously finding ways around the cybersecurity controls that we implement. This is why we must establish versatile and dynamic cybersecurity programs that are able to adapt as threats evolve. While we still need to set alarms and monitor for anomalous events, we also need to lock the cybersecurity doors. One way to begin accomplishing this, is through a strong Vulnerability Management Program that incorporates diligent patch management.

We hear security professionals talk about Zero-Day threats, in which vulnerabilities or weaknesses in systems, unbeknownst to the vendor, are exploited by hackers. However, while these risks requires proper controls, the most publicized attacks this year, affecting hundreds of millions of people, were due to exploiting known vulnerabilities. As these attacks were not Zero-Day, they were completely preventable.

- Equifax Data Breach – The Equifax breach that exposed over 143 million American's personal and financial records was due to an exploit of an Apache Struts vulnerability, identified in early March of 2017. A patch was made available shortly thereafter. According to CNN Tech's Jackie Wattles and Selena Larson, "Equifax admitted it was aware of the security flaw a full two months before the company says hackers first gained accessed to its data." (CNN Money)

- WannaCry Ransomware - In May, 2017, WannaCry Ransomware affected Windows machines worldwide. Microsoft had identified the vulnerability, and released a patch as part of the Microsoft MS10-017 updates in March, two whole months before the exploit spread like wildfire.

- Petya Ransomware – A little over a month after WannaCry, this second ransomware attack was unleashed on the world, also exploiting a vulnerability that was addressed in the Microsoft MS10-017 update.

According to the March 14, 2017 article in eWeek magazine entitled, "Software Patches Could Prevent Most Breaches, Study Finds," "Approximately 80 percent of companies that had either a breach or a failed audit could have prevented the issue with a software patch or a configuration change, according to a security-automation survey of 318 firms."

"Approximately 80 percent of companies that had either a breach or a failed audit could have prevented the issue with a software patch or a configuration change, according to a security-automation survey of 318 firms."

-eWeek magazine "Software Patches Could Prevent Most Breaches, Study Finds"

There are many reasons why firms fail to adequately patch their systems, some of which include:

- Rogue systems, or systems that were seemingly decommissioned, remain on the network.
- Organizations do not know that their systems' patches are not current.
- Organizations do not have the resources to properly test and deploy patches.
- Legacy systems may break if patches are applied, and engineering fears unforeseen business repercussions due to unplanned downtime.
- The business requires 100% uptime and does not allow for Change Management Windows to patch.

The development and implementation of an adequate Vulnerability Management Program, with proper patch management policies and processes, are key to addressing the above challenges. The following are helpful steps towards establishing such a program:

- As with any cybersecurity program component, support from your senior management is key. Involve executive management, and emphasize that the cost of a breach far outweighs the cost of implementing the program.
- Identify business requirements and risks caused by downtime. If the business requires 100% uptime, implementing high availability systems can allow for patching without incurring down time.
- It is impossible to protect what you do not know. It is therefore imperative to fully inventory an organization's cybersecurity assets, including anything with an IP address (infrastructure devices, servers, endpoints, appliances, phones, etc.), and applications that run on those assets.
- Implementing a vulnerability scanning solution, that continuously scans the environment, will identify all assets that can be compared with the asset inventory above, and the vulnerabilities of those assets.
- Prioritize patching based on the proportion of the asset risk to the business.
- Implement set Change Management Windows for the purpose of patching.
- Where legacy systems cannot be patched, identify compensating controls to mitigate the risk.
- Being that one of the biggest issues most firms face is time and engineering resources, do not go it alone. Utilize outside expertise to enhance your organization's current team.

While a crook will find a way, do not make it any easier. Lock your cyber doors and significantly reduce your risk exposure by implementing and maintaining a good Vulnerability Management Program, that includes consistent and prioritized patching.

About the Author

Seth Arbital, Chief Information Security Officer of Align

Seth Arbital draws from his 30 years of experience in IT and 15 years specializing in Information Security as the CISO of Align. Seth has built and managed consulting and engineering teams for boutique, regional and national technology firms. He assists clients in enhancing security by developing strategic security programs with a focus on people, process and technologies. Seth utilizes his expertise with security technologies, architect's solutions and manages business and regulatory compliance including PCI, HIPAA, GLBA, and SOX. He is certified in CISM, CISSP, ISO 27001 and GDPR, as well as a variety of technical certifications from security vendors. Seth received his Bachelor of Science in Computer and Information Sciences at City University of New York – Brooklyn College.

ABOUT ALIGN

Align specializes in strategy, design, deployment, optimization and transformation of your technology infrastructure. Since 1986, the world's leading firms have relied on Align to guide them through IT challenges, delivering complete solutions for business change and growth. Our proactive process enables businesses to evaluate technology initiatives and resource constraints and develop results-oriented plans. We employ industry best practices to help clients set priorities, design a realistic schedule and budget and guide multiple projects to completion. With over three decades in the field, we have created a series of robust tools and custom dashboards to review and manage key metrics and details. These tools and dashboards improve transparency and control, mitigating risk and enabling us to execute projects with consistency and reliability, thus reducing uncertainty in all phases of our clients' projects.

How We Can Help

Align is a Microsoft Gold-Certified partner, providing cutting edge services to help businesses optimize operations and bolster security to drive maximum efficiencies across your business. With Align and Microsoft, we can help you take your business to the next level with our cloud services, flexible IT and advanced software.

Align Cybersecurity™

Align Cybersecurity™, the first comprehensive cybersecurity risk management solution, was designed to defend against and preempt sophisticated attacks, as well as discover your firm's greatest vulnerabilities. Align offers a customized cybersecurity program, which will assess and update your current policies and provide best practices. Additionally, Align will evaluate your current risk profile and perform periodic penetration testing to understand real time threats. Advanced employee education modules on risk, threats, mitigation and remediation, as well as testing and retraining, were developed to empower staff with knowledge and awareness so they can become your greatest line of cyber defense. Your personalized cybersecurity program can be managed seamlessly with a centralized client-dedicated portal.

For more information about our services, contact cyber@align.com or visit www.aligncybersecurity.com.

Cover Image Source: "Global Access Can Also Mean Global Cyber Crime." *U.S. Air Force*. N.p., 01 Oct. 2014. Web. 01 Dec. 2017. U.S. Air Force.