RIA WorkSpace

# KEEPING RIAS SAFE

## COMBATING CYBERCRIME ON AN SMB BUDGET

WWW.RIAWORKSPACE.COM
877.415.0059
INFO@RIAWORKSPACE.COM

# WHAT HAPPENS ON MAIN STREET STAYS ON MAIN STREET

When security breaches happen on a large scale to big business, it makes headlines. Yet little is mentioned when cybercrime hits small to medium sized businesses (SMBs). Very few people are even aware that today's cybercriminals are targeting smaller organizations, not just supersized global businesses.

According to Ponemon's 2017 State of Cybersecurity in SMBs, 61% of respondents experienced a cyber attack and 54% had data breaches - up from 55% and 50% in 2016. 72% of successful data breaches happened in smaller companies.

# EVERYONE IS A VICTIM WHEN IT COMES TO CYBERCRIME

The loss and exposure of confidential data from a cyber-attack is costly to both the people victimized and the businesses whose data was compromised.  For the victim, hackers typically retrieve identifiable personal information, bank account, credit card, financial information, and social security numbers, resulting in identify theft and financial fraud. The stress and time involved to reclaim their identity and get their financial house back in order is beyond measure.

For businesses, there are 47 state-specific DBN (Data Breach Notification) laws in the United States. Adding to the complexity and costs of this process is the fact that laws and compliance obligations vary from state to state. A breach of customer data in Pennsylvania will have different breach notification and follow-up requirements than a breach involving a customer in Massachusetts. This means firms servicing customers and clients from more than one state are responsible for these duplicate legal, regulatory and compliance burdens.  As an RIA, you know that the SEC has clear guidelines of your responsibilities in the area of security and data protection.

# CYBERCRIME COMES AT A HIGH PRICE FOR RIAS

The trend of cybercriminals preying on smaller businesses doesn't seem to be waning. According to the Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses report, the percentage of small businesses that have experienced a cyber attack in the past 12 months is up from 55% in 2016 to 61% in 2017. The average cost per breached record in the US was $225 for 2017 and the four-year average was $216.

According to Small Business Trends, in 2017 more than 72% of successful data breaches happen in smaller companies. About 71% of small business owners admit to lacking confidence in their current cyber security measures.

This amount factors in the costs of the investigation and notification process, fixing the issue that led to the breach, possible liability and litigation costs, lost business, and the time and effort that go into damage control. In many cases, a damaged reputation may prove to be irreparable. Nearly two-thirds of victimized companies are out of business within six months of a significant cyber-attack, making cybercrime the death knell for many RIAs. This is because the consequences of cybercrime extend well beyond the actual incident and have long-lasting implications.

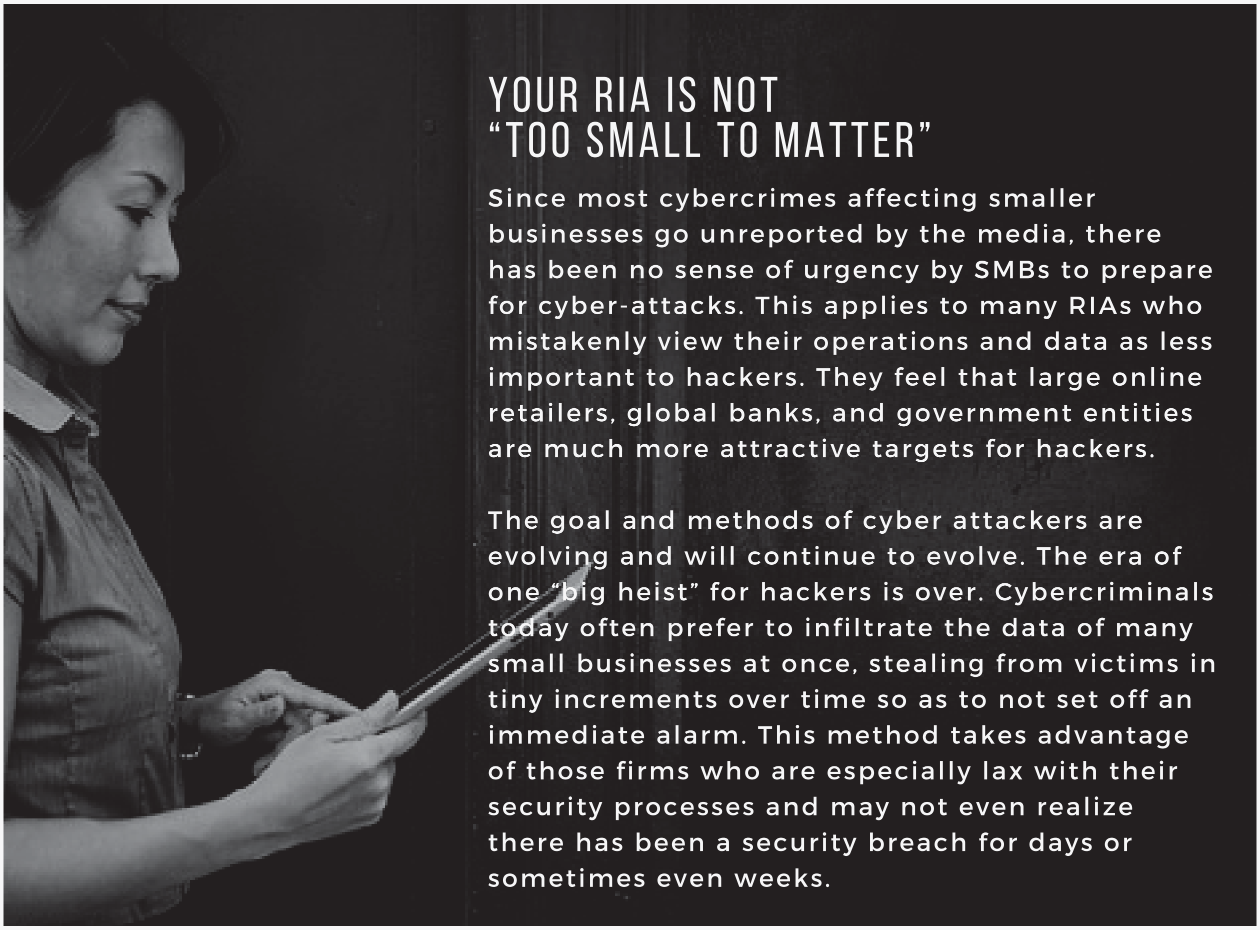
Symantec's research found that customers affected by security breaches are generally less forgiving of smaller businesses than larger companies. A small or mid-sized RIA is contending not only with lost time and revenue as well as increased expenses, but t more importantly the trust of clients and business partners.

And yet, sadly, 69% of Americans think having their personal information stolen in their lifetime is inevitable – and 84% feel their personal information is more vulnerable than it was a year ago, according to a new survey by Wakefield Research for Citrix.

# WHY CYBERCRIMINALS ARE ZEROING IN ON SMBS

Large corporations have the resources to invest heavily in sophisticated security strategies to stop most cybercrime attempts. A typical large enterprise may have over twenty in-house IT employees ensuring that every device connecting to their network is adequately protected.  However, a shortage of cybersecurity skills is common amongst SMBs.  In 2018, 51% claimed their organization had a shortage of necessary skills to completely combat cyber crime.

Smaller RIAs usually lack the resources of large enterprises and can't afford to build the same level of security in house. Very few RIAs have full-time IT dedicated personnel on hand to run routine security checks. Even those who do have in-house IT support often find that their internal resources are too bogged down with other tasks to properly address security upkeep.



## YOUR RIA IS NOT "TOO SMALL TO MATTER"

Since most cybercrimes affecting smaller businesses go unreported by the media, there has been no sense of urgency by SMBs to prepare for cyber-attacks. This applies to many RIAs who mistakenly view their operations and data as less important to hackers. They feel that large online retailers, global banks, and government entities are much more attractive targets for hackers.

The goal and methods of cyber attackers are evolving and will continue to evolve. The era of one "big heist" for hackers is over. Cybercriminals today often prefer to infiltrate the data of many small businesses at once, stealing from victims in tiny increments over time so as to not set off an immediate alarm. This method takes advantage of those firms who are especially lax with their security processes and may not even realize there has been a security breach for days or sometimes even weeks.

## THE ACCESS RAMP TO BIGGER & BETTER DATA

One reason small RIAs are more vulnerable is because they offer an inroad to larger better-protected entities. They are often sub-contracted as a vendor, supplier, or service provider to a larger organization. This makes RIAs an attractive entry point to access the data of larger companies.

Since larger enterprises have more sophisticated security processes in place to thwart cyber-attacks, smaller RIAs often unknowingly become a Trojan horse used by hackers to gain backdoor access to a bigger company's data. There is malware specifically designed to use a website as a means to crack the database of a larger business partner.
For this reason, many potential clients or business partners may ask for specifics on how their data will be safeguarded before they sign an agreement. Some may require an independent security audit be conducted. They may also ask RIAs to fill out a legally binding questionnaire pertaining to their security practices.

An RIA that is unable to prove they're on top of their infrastructure's security could lose out on potentially significant deals and business relationships. Many large enterprises are being careful to vet any business partners they're entrusting their data to.

# TO STAY SECURE, A GOOD DEFENSE IS THE BEST OFFENSE

RIAs must understand that the time has come to get serious with their security. SMB security spending is increasing, but confidence in being able to avoid breaches remains low.  Cyren and Osterman Research report 2017 states that 63% of SMB IT managers have increased security spending by about 27% but less than half of those believe they can prevent data breaches and protect against threats. There appears to still be a disconnect between security needs and IT staff dedicated to cybersecurity.

Cybercrime is only one cause of compromised data. There are 3 primary causes of breached security at businesses according to Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses report 52% of data security breaches are caused by acts of malicious or criminal intent. Human error (24%) and system failure (24%) account for the rest.

Data breaches aren’t always about bad people doing bad things. Many are the result of good employees making mistakes or of technology failure. RIAs don’t necessarily need a large budget or dozens of employees to adequately protect sensitive data.

A secure environment is possible even on a budget. Here are a few steps to improving data and network security.

## STEP 1: KNOW ALL DEVICES CONNECTING TO YOUR NETWORK

BYOD is becoming the rule instead of the exception for many organizations. Gartner predicts that by 2018, 70 percent of mobile professionals will use personal devices for work-related activities. So rather than trying to ban them, develop and follow through on a BYOD protocol.

Keep a frequently updated list of every device that connects to your network. This inventory is especially important given today's BYOD (Bring-Your-Own-Device) workplace where employees can access your network through several different devices. Knowing what these devices are and ensuring they're all configured properly will optimize network security.

All it takes is a regularly scheduled review to add or remove devices and affirm that every endpoint is secure. Much of this process can be inexpensively automated through a Mobile Device Monitoring (MDM) tool. Requiring an MDM technology will create separation between company and employee information.  It will approve or quarantine any new device accessing the network, enforce encryption settings if sensitive information is stored on such a device, and remotely locate, lock, and wipe company data from lost or stolen devices.

## STEP 2: EDUCATE & TRAIN EMPLOYEES

Every employee should participate in regular general awareness security training. This will not only reduce security breaches directly tied to employee error or negligence, but also train employees to be aware of and on the defense against cybercrime. Employees are critical to your security success and the prevention of data breaches. Hackers commonly break into networks by taking advantage of unknowing employees. Phishing attacks (61% of threats in 2017) – legitimate looking emails specifically crafted to mislead recipients into clicking a malicious link where they're asked to provide their username and password – are still successfully used by hackers to capture login credentials.

If a large company makes the news for a data breach tied to an infected email, be sure to share that news with employees with a warning. Come up with fun ways to teach employees how to identify spear-phishing email attempts and better secure their systems and devices.

It is also important to have a security policy written for employees that clearly identifies the best practices for internal and remote workers. For example, password security is critical and passwords should be frequently updated to a combination of numbers, lower case letter, and special characters that cannot be easily guessed. Security policy training should be integrated into any new employee orientation. This policy should be updated periodically. More important than anything, this security policy must be enforced to be effective.

## STEP 3: PERFORM AN AUDIT OF SENSITIVE BUSINESS INFORMATION

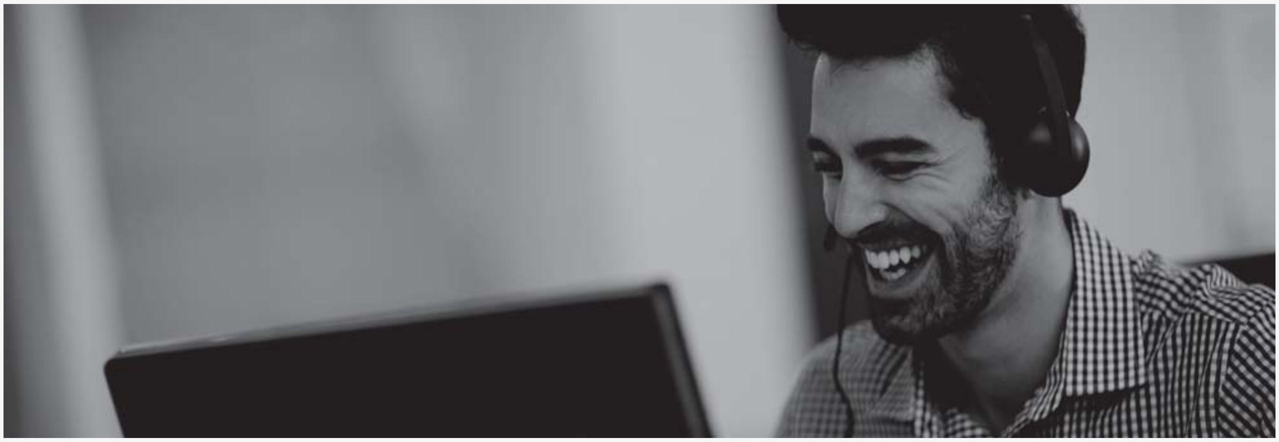
If you want to keep your most sensitive business information secure, it's important to know exactly where it's stored. A detailed quarterly audit is recommended.

## STEP 4: USE CLOUD AND MANAGED SERVICE PROVIDERS

Overall, the cloud is a more secure data solution for smaller RIAs. Any conception that the cloud isn't safe is outdated. Most of today's security breaches are a result of lost or stolen devices, printed documents falling into the wrong hands, and employee errors leading to unintended disclosures. It's fair to speculate that many of these breaches wouldn't have occurred had this information been stored in the cloud rather than computers, laptops, and vulnerable servers.

RIAs with limited budgets are actually enhancing their security by moving to the cloud. Since there is no way a smaller RIA can match a large enterprise's internal services, moving services like emails, backups, and collaborative file sharing to the cloud not only reduces total-cost-of-ownership, but gives access to top-level security to better defend against internal and external threats.

Meanwhile, a Managed Service Provider (MSP) can assume responsibility for security measures like the administering of complex security devices, technical controls like firewalls, patching, antivirus software updates, intrusion-detection and log analysis systems.
MSPs are also capable of generating a branded risk report for any potential client or business partner reviewing your security measures. This third-party manual assessment of your network security can instill confidence in prospective business partners by proving to them that any possible security risks or vulnerabilities will be properly managed and addressed.



# ABOUT RIA WORKSPACE

## SERVING ALL THE IT NEEDS OF YOUR RIA - AT ONE PREDICTABLE PRICE

RIA WorkSpace is dedicated to providing RIAs with exceptional IT support and service.  our Custom Cloud and Managed IT Platforms are perfect for RIAs that want a one-stop shop for everything IT.  Our service plan makes it easy to manage your IT budget with a fixed monthly fee, improve the reliability of your IT systems, and feel secure knowing the platform is customized for your industry.

### A DEDICATED, ASSIGNED TEAM WITH FANATICAL SUPPORT

The RIA WorkSpace team is friendly, helpful, and understand your industry.

### TROUBLE-FREE BACKUP AND DISASTER RECOVERY

Feel confident knowing your emails, files, and apps are backed up and recoverable in the event of a disaster.

### SIMPLIFIED AND RELIABLE DAY TO DAY OPERATING

With files, storage, hosted Office 365 email, and the Microsoft Office Suite, your team works with tools they know from wherever they work.

### COMPREHENSIVE SECURITY AND COMPLIANCE

Our plans are built on the unique security and compliance needs for your industry.