Technology and Cybersecurity 2022: Trends & Best Practices

RIGHTSIZE SOLUTIONS

Visory

MEET OUR SPEAKER

WES STILLMAN

Chief Technology Officer

- **30 years** in IT/Cybersecurity field
- **Founded** RightSize Solutions in 2002
- **Expansion:** Financial Services Focus

Affiliated Firms

RIGHTSIZE SOLUTIONS

SWIZZNET HOSTED ACCOUNTING SOLUTIONS

straight answers + bright solutions
TRUE NORTH NETWORKS

Visory

WHY INVEST IN CYBERSECURITY?

You're here for a reason ...

Important Motivating Factors

You've read about attacks, and you are concerned about the future.

You're concerned about regulatory standards.

You have had a close call or are recovering from a breach or attack.

RIA INDUSTRY TRENDS

96%

Financial advisors agree that technology plays a critical role in their practices

68%

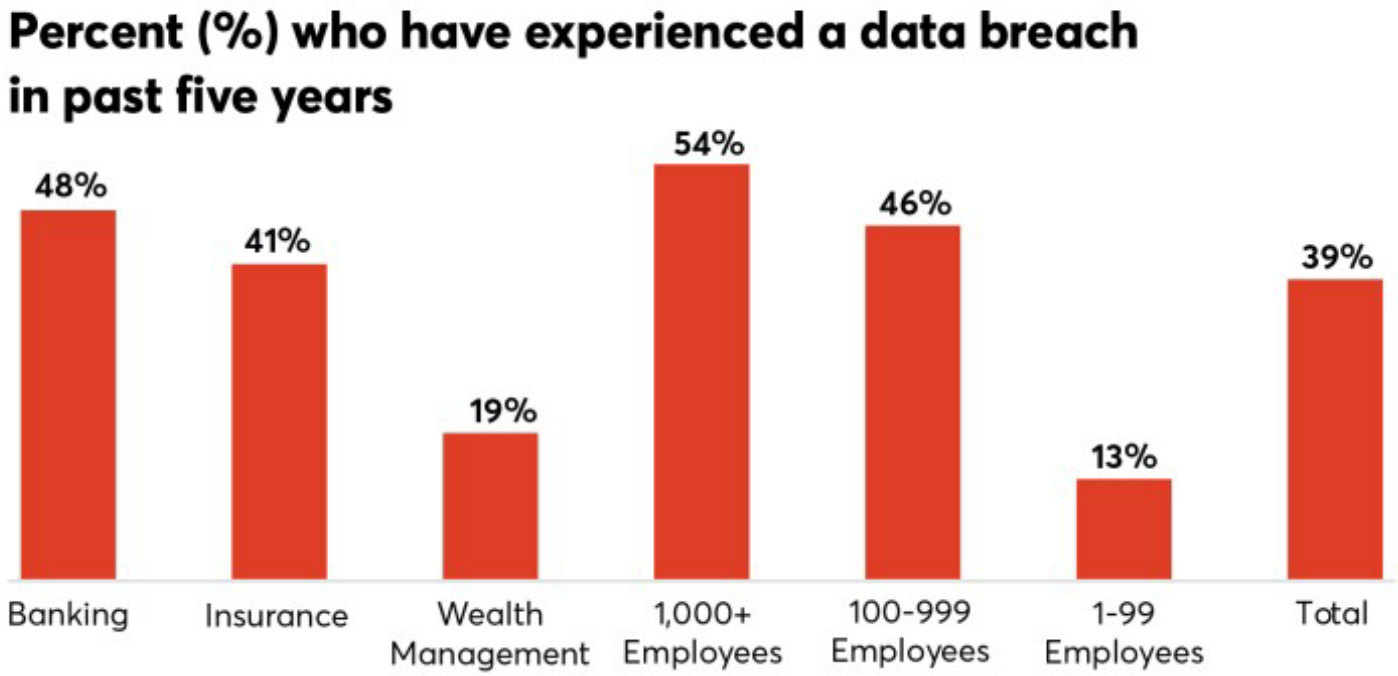
Firms prioritized spending on technology over other business needs

38%

Financial advisors are confident that they've made the right decisions in regards to new tech

What advisory firms should be doing on cybersecurity, quoting Arizent.com | Financial Planning | April 4, 2022

RIA INDUSTRY TRENDS



Wealth managers are seeing a lower rate of hacking, phishing and digital attacks than other financial services firms, but new data shows the industry has fallen behind in terms of beefing up cybersecurity.

- What advisory firms should be doing on cybersecurity | Financial Planning | April 4, 2022

RIA INDUSTRY TRENDS

High Premiums For Financial Services

The financial services sector ranks second only to payment processing companies for the cost of cyber insurance. Average annual premiums for $1 million of cyber liability insurance are shown below by industry.

Source: Advisor Smith • Created with Datawrapper

Financial services had the second highest annual cyber insurance premiums by industry in 2021, averaging $2,429 for $1 million in cyber liability coverage.

RIA INDUSTRY TRENDS

Percent (%) who have adopted cybersecurity safeguards

	Wealth management	Insurance carriers	Banking	Total
Routine vulnerability assessments	51%	49%	55%	**53%**
Routine hacks of your own systems	21%	32%	54%	**40%**
Annual cybersecurity reviews	58%	46%	53%	**53%**
Third-party vulnerability assessments	55%	46%	52%	**52%**
Immediate implementation of security patches	57%	56%	49%	**53%**
Periodic breach simulations	34%	37%	47%	**41%**
Restricting external access during security patches	28%	46%	35%	**35%**

Source: Arizent State of Cybersecurity Survey 2022

Advisory firms with small or even solo teams should also take a cue from star athletes who perform well under pressure, in part because they have rehearsed many of the clutch circumstances in practice sessions for years.

What advisory firms should be doing on cybersecurity | Financial Planning | April 4, 2022

Cyberattacks by the Numbers

Consider the hidden costs of cyberattacks:

- Firm reputation
- Client trust
- Opportunity costs
- Damaged morale
- Downtime

42%
Business & Professional Services

91%
Phishing

$150
Cost per record

3x
Triple the attacks since 2018

Ponemon Institute & IBM Security report, “Cost of a Data Breach”
Top cyberthreats targeting accounting firms, *Journal of Accountancy*, March 16, 2020

IMPORTANT REGULATIONS

What's new?

Have a plan in place for all regulations

IRS:

Publication 4557 requires professional tax preparers to create and enact security plans to protect client data.

FINRA:

Proposed 3-year pilot program for remote office inspections. Extends the online supervision of branch and non-branch operations that FINRA allowed during the pandemic.

SEC:

Proposed amendments to enhance and standardize disclosures regarding cybersecurity, risk management, strategy, governance.

GROWING NEED FOR CYBERSECURITY

What is driving it?

- The attacks themselves
- State and Federal Regulations
- Cybersecurity insurance industry
- Custodians, Broker-Dealers

SaaS AND THE EMERGING REMOTE WORKFORCE

What Does it Mean for you?

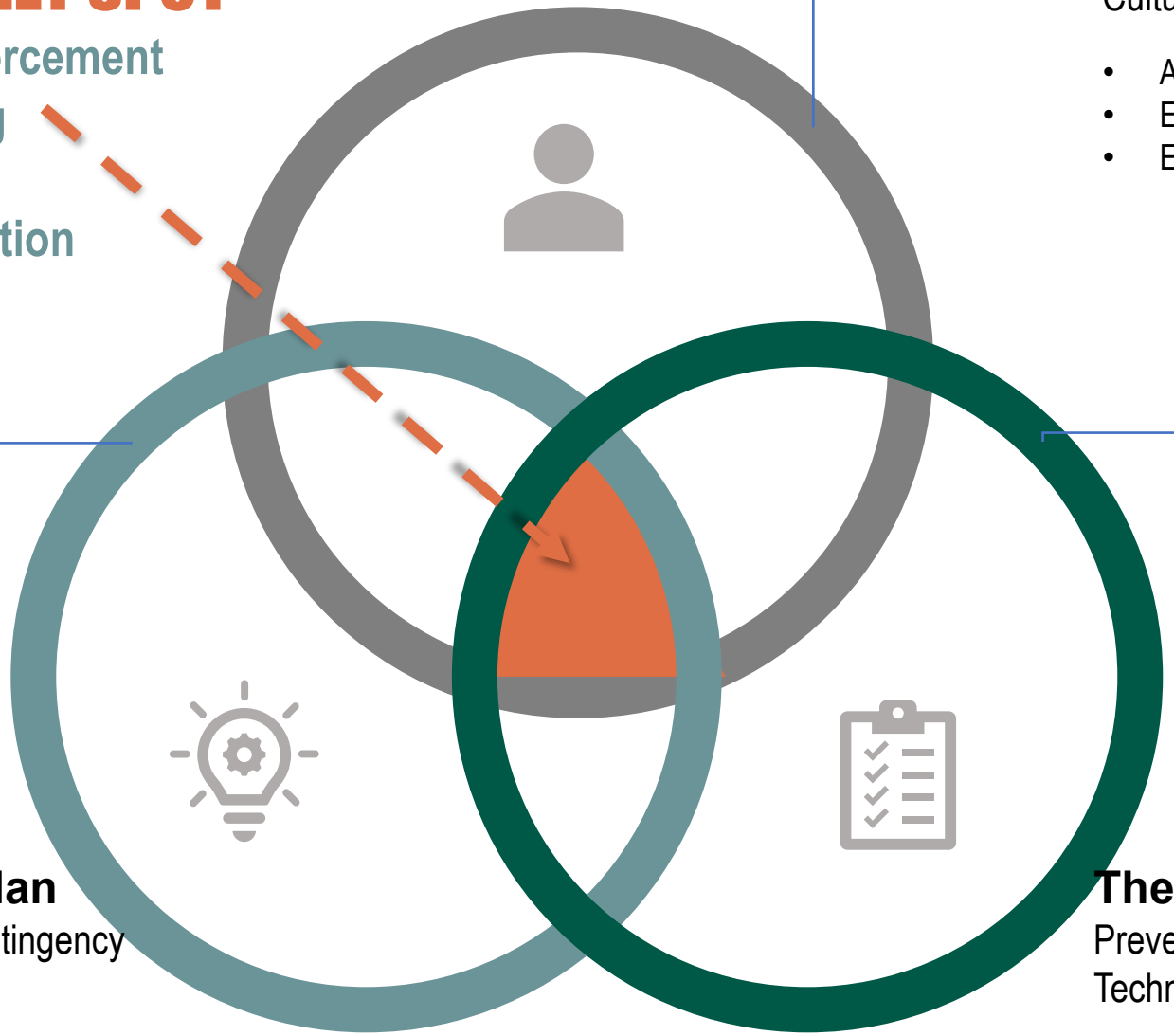
- Software vendors are enabling the move to SaaS
- SaaS makes the remote workforce a real option
- Your security policies must address this change
  - How do we access software (BYOD)
  - Anytime, anywhere access

WHERE CAN YOUR FIRM IMPROVE?

THE SWEET SPOT

Policy Enforcement

- Training
- MFA
- Preparation



1. The Human Factor

Culture of Awareness

- Awareness training
- Expect human behavior
- Enforce policies

2. The Arsenal

Prevention & Detection Technology

- Set your software foundation
- Protect your data
- Control access points
- Compliant devices

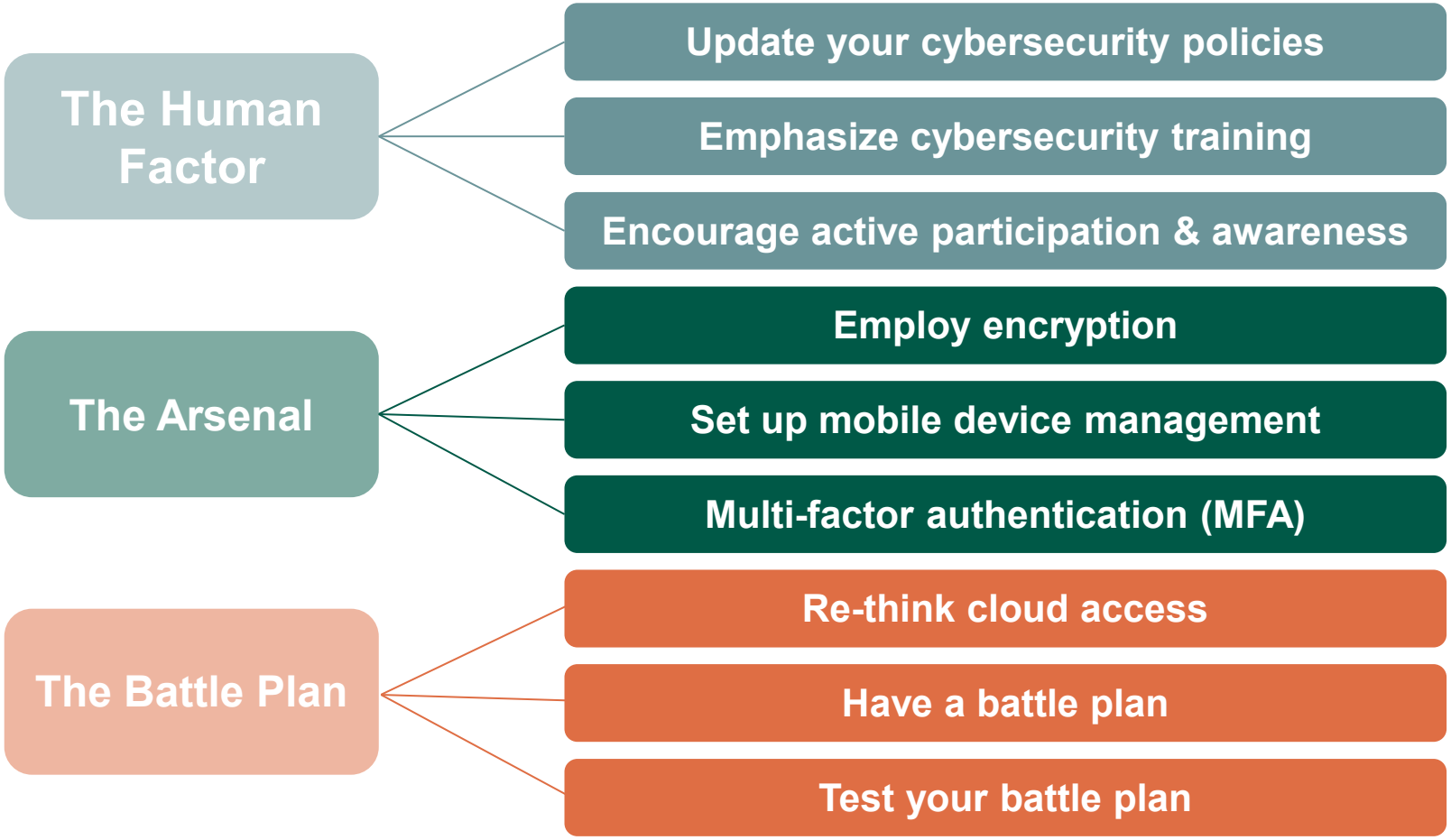
3. The Battle Plan

Preparation & Contingency Planning

- Backup your data
- Create a disaster readiness plan
- Set standards for communication
- Cyber insurance

WHAT YOU NEED TO DO TO IMPROVE THE SECURITY OF YOUR FIRM

Start by surveying your technology environment



New Year New Rules New Game

"Skate to where the puck is going, not where it has been."

-Wayne Gretzky

You don't need to be Wayne Gretzky to see where the RIA industry is going…

Create your ideal environment starting with the right:

1. Policies
2. Processes
3. Technology

To empower risk reduction and protect your firm.

THANK YOU!

Visory

14425 College Boulevard,
Ste 150
Lenexa, KS 66215

(913) 396-4600

info@rightsize-solutions.com

Stop by our booth and pick up your copy of the

10 Tips to Keep your Firm Safer