The Growing Threat

Cyberthreats and criminals ARE becoming more sophisticated and plentiful every day

Small businesses are prime targets for today's attacks

Security is more complex AND HAS TO PROTECT MORE than ever

It Could Happen to Your Business

Phishing Attack Exposes Patient Data from Colorado Healthcare Company

Florida City Pays $460,000 in Ransom After Attack

Fraudulent Bank Activity by Cyber Thieves Causes Startup to Close its Doors

67% of SMBs have experienced cyberattacks

What Do We Mean by Cybersecurity?

Cyber security is the technology, people, and processes needed to protect an organization's digital assets, including devices, software, networks, user credentials, sensitive data, transactions, intellectual property, and more against today's advanced cyber threats.
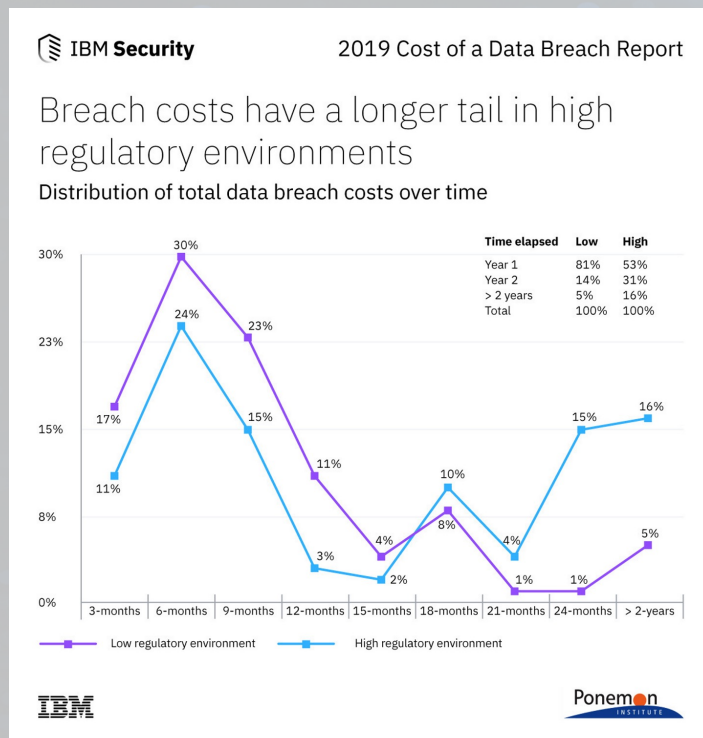
How is Cybersecurity Different than Managed IT Services?

While managed IT services can include security such as antivirus software, firewall management, and email encryption. Today they only capture a fraction of the critical cybersecurity controls needed to protect business.

What Do You Need to Protect?

The Harmful Impacts of a Significant Attack

IBM Security — 2019 Cost of a Data Breach Report

Breach costs have a longer tail in high regulatory environments
Distribution of total data breach costs over time

Time elapsed	Low	High
Year 1	81%	53%
Year 2	14%	31%
> 2 years	5%	16%
Total	100%	100%

- 63% of SMBs believe that a successful cyberattack could lead to short- and long-term business losses.

- 48% of SMBs said that a major data breach would likely *shut down* their business permanently.

- After a successful data breach, SMBs suffered **$1.43 million in damages or theft on average**, a 33 percent increase from 2017.

Security isn't a problem to solve, it's a risk to be managed.

3 Ways to Treat Risk

✔ Accept

↗ Transfer

🔒 Remediate

Sharing is generally not recommended

How can we start reducing your security risk?

The NIST Cybersecurity Framework

CYBERSECURITY FRAMEWORK

IDENTIFY · PROTECT · DETECT · RESPOND · RECOVER

69% OF SMBs — HAVE NOT identified & documented cybersecurity **THREATS**

66% OF SMBs — HAVE NOT identified & documented cybersecurity **VULNERABILITIES**

57% OF SMBs — HAVE NOT informed & trained all users on **CYBERSECURITY**

48% OF SMBs — HAVE NOT analyzed cybersecurity attack **TARGETS & METHODS**
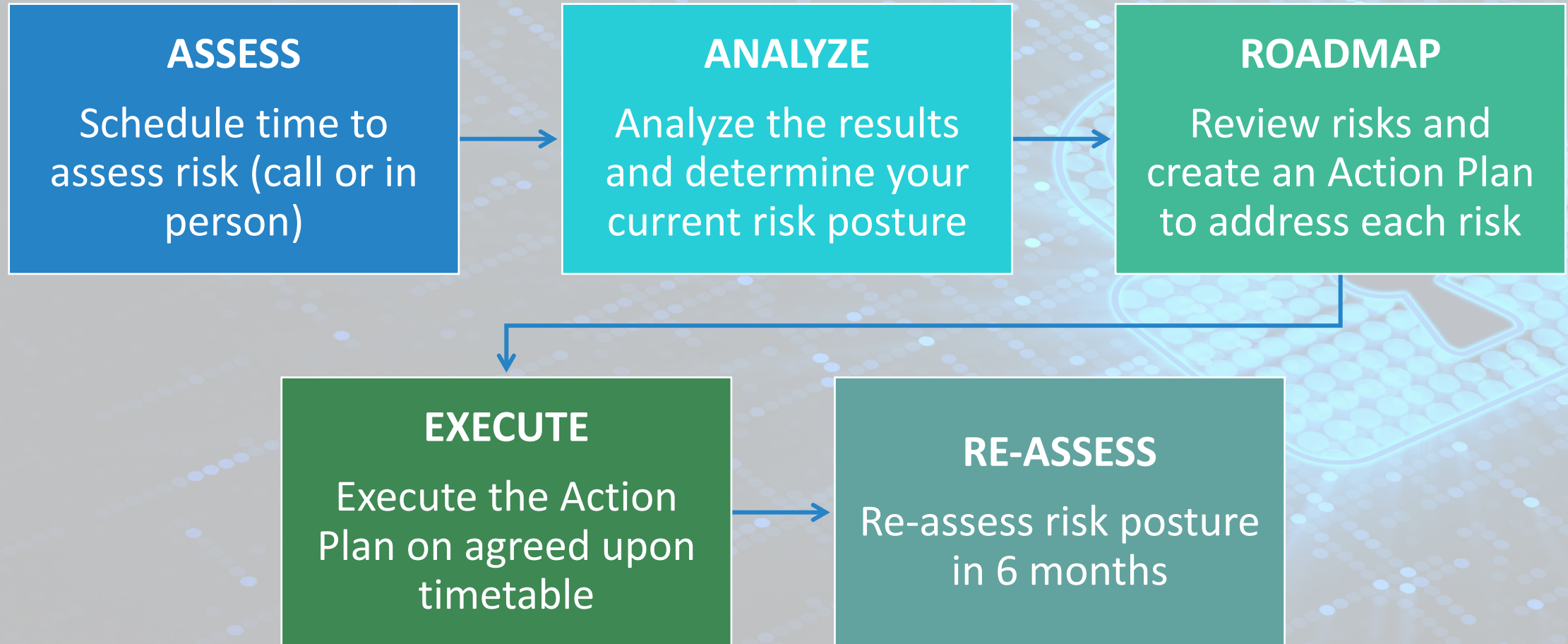
48% OF SMBs — DO NOT have a **RESPONSE PLAN** for a cybersecurity incident

43% OF SMBs — DO NOT have a **RECOVERY PLAN** for a cybersecurity incident

*Based on anonymous data of over 1,000 risk assessments, March 2019

Our Approach to Assessing Your Risk

ASSESS

Schedule time to assess risk (call or in person)

ANALYZE

Analyze the results and determine your current risk posture

ROADMAP

Review risks and create an Action Plan to address each risk

EXECUTE

Execute the Action Plan on agreed upon timetable

RE-ASSESS

Re-assess risk posture in 6 months

The Right Action Plan

Cybersecurity Action Plan

We've taken the results of your cybersecurity risk assessment and developed an action plan to address your risks in phases to fit your timeline and budget.

Phase 1

Timeframe: i.e., Q4

Risk Area	Risk Level	Remediation Action & Product Recommendations	Start Date	End Date	Hours	Cost
i.e., Response plan is executed during or after event	High	i.e., Develop a disaster recovery response plan	10/1	10/30	7	Included
		i.e., implement backup testing solution [insert product]	10/1	10/30	10	$1,250
				Total Cost		

Notes

Let's Discuss Next Steps

Contact WI-Tech CyberSecurity

Phone: 832.553.6404

Email: HelpDesk@WITechCyberSecurity.com