Could a Cyberattack Put You Out of Business?

Understanding Today's Increasing Security Risks for Small and Medium-Sized Businesses

Phone: (888)-642-8472

Email: info@verity-it.com

Website: verity-it.com

The Growing Threat

FACT: 67% of SMBs have experienced cyberattacks.

Cyberthreats and criminals are becoming more sophisticated and adapting more everyday.

With a rapid growth of online criminals, they are quickly figuring out how to bypass and navigate the basic security measures, putting your business at a higher risk.

Small businesses are prime targets for today's attacks.

Cyber criminals have a tendency to target small businesses because they know bigger companies have the resources to invest more on security measures. They are placing their bets that a small business is less likely to be as protected.

Security is more complex and has to protect more than ever.

While security practices have become more complex with layers of protection to evade any type of attack, there's a lot more to protect than ever before. Your company has more data, more apps in the cloud and more mobile devices that all require consitent protection.

What Do We Mean by Cybersecurity?

Cybersecurity is the technology, people and processes needed to protect a company's digital assets (devices, software, networks, user credentials, sensitive data transactions, intellectual property and more) against today's advanced cyberthreats.

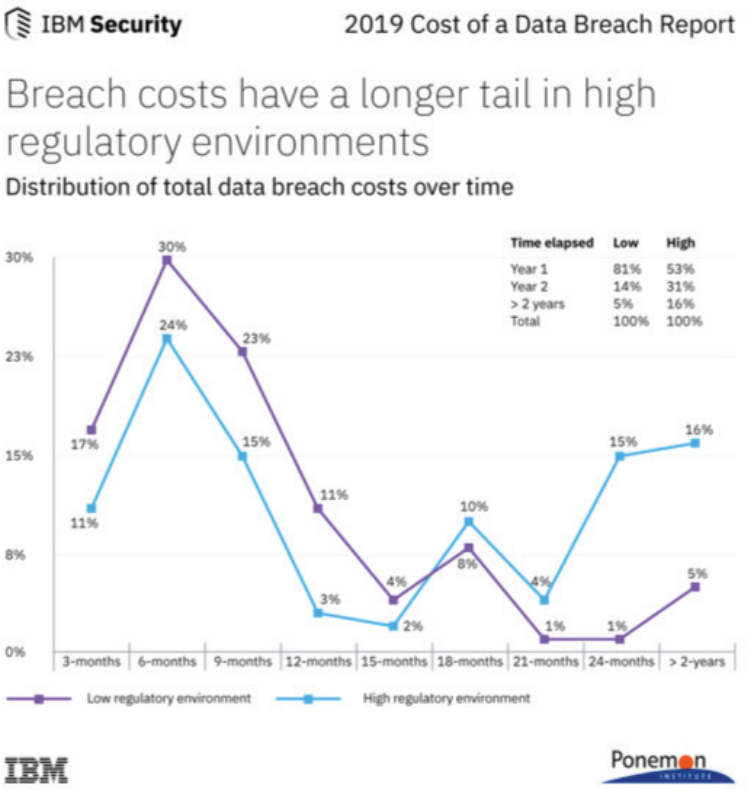
How Is Cybersecurity Different Than Managed IT Services?

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 businesses. Security can also include physical security of your business facility, protecting against unauthorized access.

The Harmful Impacts of a Significant Attack

- 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 completely.



1. AppRiver Cyberthreat Index for Business Survey. https://www.appriver.com/files/documents/cyberthreatindex/AppRiver-Cyberthreat-Index-for-Business-Survey-exec-summary_FINAL.pdf

Times were much more simple when a software virus only effected one employee and they weren't able to use their computer for a while. Not so much today – cyberattacks are a lot more brutal, long-lasting and destructive. The financial, operational and reputational repercussions are unbearable along with the potential for non-compliance penalties for companies in regulated industries like healthcare and financial services.

The result is that nearly a third of SMBs believe that a successful attack could lead to business losses, with almost half of SMBs believing that they would potentially close their doors permanently in the event of a significant attack. And while the costs of recovery, lost customer trust and business, work stoppage, and more vary, the average amount of damages continues to escalate dramatically each year.

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

How Can We Start Reducing Your Security Risk?

What can you do as a small business to protect your assets? It's important for you to first understand what risk your business faces and your risk exposure.

We are able to help identify your greatest areas of risk for a security data breach. Keep in mind that the most critical risks are not only with your IT enviornment, but in the processes, policies and procedures that can leave you open to popular phishing and social engineering attacks.

3 Ways to Treat Risk

ACCEPT

You can accept it and not take action. You might do this if the risk is minimal and unlikely to cause serious damage to your business.

TRANSFER

You can transfer the risk to another entity, like Verity IT, for example.

REMEDIATE

You can remediate the risk by implementing practices to reduce or eliminate cyberattacks. This is suitable when the risk cannot be accepted, avoided or transferred.

The NIST Cybersecurity Framework

The NIST cybersecurity framework is a proven approach to protecting your business. It's designed to help SMBs assess their strengths and vulerabilities while improving their security practices.

Follow the five-step framework to:

1. Identify your company assets
2. Protect those assets
3. Detect anomalies and events
4. Respond with a plan to mitigate damage
5. Recover systems and data and make improvements

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

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

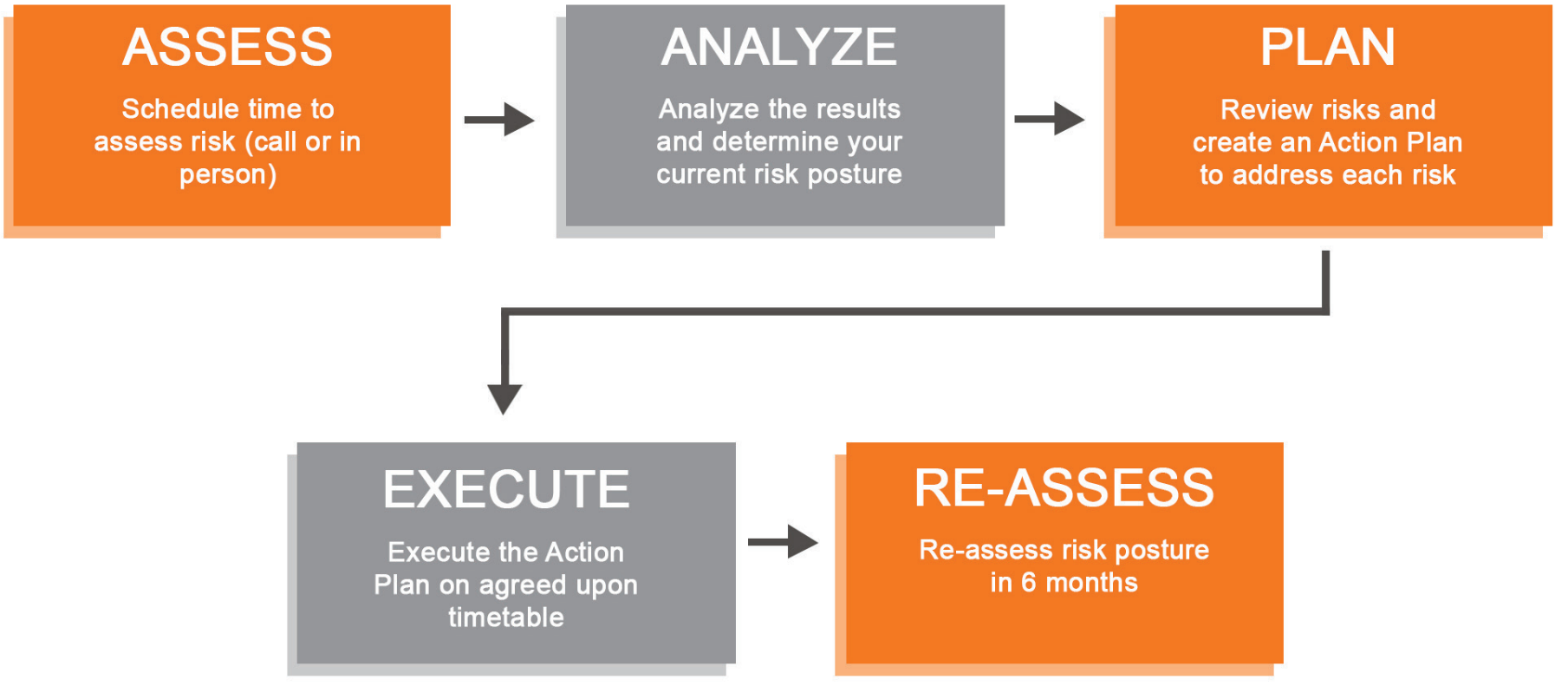
57% OF SMBs HAVE NOT informed & trained all users on **CYBERSECURITY**

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

Our Approach to Assessing Your Risk



It's important to perform a cybersecurity risk assessment of your business before a breach that makes you vulnerable. This assessment will measure your operations against the NIST Cybersecurity Framework and will determine how well prepared you are for a cyberattack.

Here's how it works:

- We interview you with questions across your current policies, procedures, and infrastructure, based on the NIST Cybersecurity Framework.
- We aggregate the findings into an easy-to-understand report showing your top security risks and the impacts they have on your business.
- We discuss the top risks and which ones are most important to you.
- We develop a plan of action that fits your timeline and budget.
- Because security risk management is an ongoing process, we re-asses your risk in 6 months to see the impact of the work we've done and what new risks may have risen.

ABOUT US

Verity IT is a full-service technology consulting partner, providing IT Consulting, Managed IT Services and Managed Security Services in Chicago. Specializing in middle market businesses, we create a plan fit for today's IT needs while still accommodating for tomorrow's growth.

Transforming operations and making businesses smarter and more efficient, our IT outsourcing model provides executives the opportunity to shift focus from managing complex and inefficient IT environments, to developing IT strategies that provide immediate return on investment. Experience lower IT costs and predictable budgeting, enhanced focus on core business operations, improved operational efficiencies and increased ability to achieve goals with Verity IT.

Phone: (888)-642-8472
E-mail: info@verity-it.com
Website: verity-it.com

VERITY

Conclusion:

We're here to help!

- **Deep Expertise and Experience**
- **Industry Knowledge**
- **Trusted Partner**
- **Full Service**
  - Managed IT Services
  - Managed Security Services
  - Cybersecurity Risk Assessment