FirstCall

WE MAKE IT BETTER!

S.H.I.T.

Security Hardening Isn't Tough

This guide was created for organizations who are vulnerable because cybersecurity has been defined as too technical, too complex or too expensive. Security hardening isn't tough and throughout this guide we will explore how to navigate your cybersecurity landscape.

ABOUT THE AUTHOR

CONOR SMITH

CEO / President – First Call Computer Solutions

Conor is a veteran of the high-tech sector in Montana and beyond. His team of over 50 IT professionals helps small and medium sized organizations implement practical yet transformative IT, security, voice and web solutions.

Conor does his best to walk with the spirit each day. Sometimes he runs too far ahead, sometimes he is caught just standing there. But he is always trying to embrace the struggle and the gifts. He is blessed with his wife and family. Loves to camp, ride motorcycles, hit the lakes and slopes. His heart is also in building a great company, right here in Montana surrounded by wonderful talented people.

TABLE OF CONTENTS

01
So, Why give a...?

02
Why security hardening feels tough

03
Prevention isn't your only focus

04
Which industries are high risk?

06
Why drives business owners to tighten security?

07
What you can do today to improve your security

08
Conclusion

So, Why give a...?

There are four primary reasons you need to consider while examining cybersecurity and your business. You will want to create an all-encompassing strategy to safeguard your company by keeping these in mind as you consider your options.

Intrusion

When an attempt is made to access your computer(s) or join a global operation, this is known as an intrusion. Although there are numerous resources available to assist in setting up defenses against this kind of activity, finding the appropriate one for you can be fairly challenging. Protecting your finances and data is your responsibility. You run the danger of losing money and being sued if you maintain any sensitive data.

Liability

With intrusions come liabilities. Organizations that collect sensitive information are held liable for the protection of that data. In order to protect your organization from increased liability, having the appropriate cybersecurity measures are critical. This becomes especially when dealing with cybersecurity insurance providers. Maintain compliance and reduce exposure to liabilities.

Business Killers

A breach or numerous attacks may lead to the demise of a company. Your total performance may be impacted by the financial pressure and risk your firm exposes you to, which may even put the future viability of the company in jeopardy.

Reputation

When a bank falls victim to a cybersecurity incident and is breach, the organization’s reputation is immediately tarnished. Customers won't believe you can protect their private information. If not a total business killer; growth and overall business success is sure to suffer.

Why security hardening feels tough:

There are a few factors that may prevent business owners from actively addressing their cybersecurity. These include:

Too technical : It is too complex to understand the depth of the audit and/or compliance standards. You need to have someone break the subject down into manageable steps and have knowledge of the subject.

Too complex: It is too complex to understand the depth of the audit and/or compliance standards. You need to have someone break the subject down into manageable steps and have knowledge of the subject.

Too expensive: The cost of implementing a cybersecurity strategy often leaves many organizations with sticker shock, more so when they do not fully understand what they are paying for. But once an organization understands where they stand and what is needed to achieve compliance, the costs become much easier to swallow. Keep in mind, being proactive is far less costly than scrambling to react to an incident.

Prevention isn't your only focus

90% of breaches are avoidable. However it's not just about prevention. When reviewing your cybersecurity measures, it's also advantageous to do think about the following questions:

- Have your assets been identified?
- Have those assets been protected?
- Can you find any unauthorized entries?
- Do you have a strategy in place to respond if you notice it?
- Can you recover if you had to respond?

You can better understand your company, it's worth, and its shortcomings by working on its cybersecurity.

Which industries are high risk?

Healthcare

In order to avoid disruptions and facilitate hospitals, clinics, or doctor's offices to access vital data from medical records and utilize the clinical equipment that may result in canceled treatments, upset patients, and even facility closures, healthcare must always be protected from attacks and leaks.

Healthcare

The financial information that can be accessed through any breach can have fatal repercussions and expose one to both legal and financial sanctions. There are also many tiers of necessary security precautions that must be put in place. Financial institutions are a prime target for ransomware attacks.

DoD Manufacturing

Your data and systems must remain secure in order for DoD manufacturing, personal safety, and national security to be preserved. A gatekeeper can be added by working with a reputable business to keep your cybersecurity protected.

Which industries are high risk?

Utilities

Today's society is supported by utilities, the delicate network of services that utility firms offer. It is crucial to keep them protected from cyberattacks and the disruptions they may cause.

Local Governments

It is crucial for local governments to maintain public access to all of their private information. Data loss or the failure of major systems like 911, police, and fire that defend your neighborhood can be devastating results of an attack or hack.

Schools

Cyberattacks can be virtually as harmful as physical assaults at school. By partnering with a qualified cybersecurity specialist, you get assistance and may focus on the important parts of your job.

Which industries are high risk?

- Another company in the industry has experienced a breach and theconsequences are now easier to understand.
- You have had a 3rd party cybersecurity audit but don't have the resources to implement the required measures.
- Cybersecurity insurance requirements are eye-opening and sometimes difficult to fully comprehend.
- Phish-testing has exposed vulnerability
- There are lingering issues with no champion to address.
- Lacking internal technical skills and not sure of a resolution.
- Alignment with nationally recognized standards has not been achieved.

What you can do today to improve your security:

- Implement tools to mitigate the impact and damage users can cause through behavioral mistakes
- Train/Test provides ongoing security awareness, training, and testing. Easy to understand, quick, and regularly reinforces the importance of protecting the organization.
- Consider co-managing to supplement roles, processes, tools, and automation that can cost less through outsourcing.
- Executive-level risk assessments are low-cost, educational, and extremely impactful in helping leaders see where they are out of alignment, helping them understand the extent of the gaps.

What are our key goals?
Bring in 4 Leads/Appts Per Month
Build KLT
Clean up site content for better sales funnel

Cyber Risk Engagement Sessions

Understand the technical, behavioral and hard costs associated with shoring up cybersecurity

FirstCall

WE MAKE IT BETTER!

Managed IT & Security | Websites | Voice | IT Projects

Schedule One TODAY

Leverage our knowledge with organizations and industries across Montana.

We have affordable, practical and impactful approaches whether you have an internal IT department or currently use a 3rd party Managed Service Provider.

Conor Smith CEO
csmith@firstsolution.com