What You Should Be

Asking Your IT Company About Cybersecurity

As many businesses around the world continue to fall victim to cyber attacks, it's important now more than ever to reevaluate and potentially add to any protective measures already in place. Current cybersecurity measures are critical, as more than 60% of small businesses go out of business within six months after being hacked.

Traditional security measures —such as firewalls, legacy antivirus software, patch management and backups—are no longer enough of a defense against today's increasingly sophisticated and effective attacks. We're seeing extremely well-coordinated, highly targeted incidents carried out against a variety of industries, from healthcare to government to finance and everything in between. Every industry is vulnerable without adequate protection in place.

Today's threats have evolved beyond basic security measures taken by most IT companies. For example, many companies are not aware that traditional antivirus software cannot stop ransomware, which can encrypt 100% of your network and your backups in a matter of minutes. Once you are hit with ransomware, possible payouts can exceed hundreds of thousands of dollars. Beyond paying this hard dollar amount in ransom, your business could be unable to operate for weeks and sensitive information could be made public.

In order to prepare yourself for these threats, we recommend taking some time to talk with your IT company and review the tools you have in place. Preparation is key if you want to minimize risk and downtime due to a ransomware attack. To help guide that conversation, here are some questions you can talk through with your IT company:

- What proactive preventative steps are we taking to monitor and minimize the risk for a potential breach?
- What tools and resources do we have access to monitor, identify and notify us about suspicious behavior?
- Can we detect signature-based and heuristic threats?
- Are we able to detect and quarantine malware in both open and isolated networks?
- Do you provide comprehensive reporting to give us visibility into the status of our security?

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

- Do you have experience negotiating a ransom? How would we evaluate a ransom situation to determine if we should pay it?
- How long will it take us to recover from a cyber attack?
- Have we done a risk assessment of our existing systems to determine any gaps in security?
- Who is independently auditing the safety and security of the systems you installed and manage for us?
- Do we have an Incident Response (IR) plan?
- Can we go through a tabletop exercise to walk through threat scenarios?
- Do you partner with an independent and separate cybersecurity company with experience in managing breaches that could be called in if we have a crisis?
- Do we have the proper procedures in place to contain and mitigate damage while preserving evidence and complying with law enforcement requests?
- Are you willing to bring in a cybersecurity partner to work cooperatively with you to secure our system?

Given the cybersecurity talent shortage and advanced threats they and their clients face, many IT companies now offer cybersecurity as a service or as an extension of their core offerings. Progressive IT companies understand that they must have effective people, processes and tools in order to defend today’s networks, and they understand the value in partnering with dedicated cybersecurity experts as an extension of their capable team.

It is now an accepted industry best practice for IT companies to partner with cybersecurity specialists. Many IT companies are now partnered with cybersecurity specialists. However, unfortunately, there are a significant number of IT companies that still aren’t providing adequate tools, expertise and resources to mitigate potential cybersecurity threats. As the number and frequency of organized attacks increases, it’s important now more than ever to realize that today's threats call for a much more advanced, comprehensive solution.

A Trusted Advisor & Service Provider

Since 2010, Ingalls Information Security has been in the war rooms and board rooms of Global 2000 companies, investigating computer networks targeted and attacked by criminals and nation-state sponsored hackers. This experience gives us an edge in preventing and responding to cyberattacks, as well as developing risk management strategies for our clients. We work for high-profile clients in many different industry verticals, from multi-national conglomerates to small businesses that are increasingly vulnerable to cybercrime.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452