Cyber Security. Points that need to be part of the conversation

Executive Briefing

Table of Contents

1210 NE Windsor Drive
Lee's Summit, MO 64086

Introduction

Cyber security has emerged as the number one priority and if it has not for you, it should. Today's connected business world means there are thousands of entry points in and out of companies. The exploding number of access points to companies means our firewalls now have thousands of openings. What has been traditionally seen as a simple component of an organization's infrastructure – throwing a firewall and antivirus solution down as adequate has evolved into something that can keep you awake at night. The scary truth is that network security does not work as well as we thought.

It is a fact that cyber threats are continuing to increase. This increase is due, in part, to evolving external and malicious threats. Enterprises today aren't just facing a single attacker or the stereotype of a teenager in the basement just doing it to be doing it. We are fighting well-organized, well-funded adversaries who have formed a sophisticated marketplace; one that is efficient at orchestrating multiple attacks on the same targets with diverse techniques.

We can't ignore cyber security. It is an undesired event and we have to do something about it. Cyber threats are changing constantly. Threats are targeted, and they continue to get even more targeted. It used to be a virus was thrown out there and whomever it hit, it hit. Now the attackers are going after specific companies and systems trying to steal specific information or cause DoS attacks against specific systems or use networked devices as pivot points to gain access into a business network.

It's not enough for companies to ask 'Are we secure?' You need to be asking:

- ***How do we know we're not compromised today?***
- ***How would we know?***
- ***What would we do about it if we were?***
- ***Are we prepared to face the threat?***

Today there are many unpatched systems, hackers scanning for vulnerability in systems, and cyber criminals using a variety "things" every day to break into companies. And there are thousands and thousands of exposed, unprotected devices on the Internet that are inviting unwanted persons to come right in.

The topic of cybersecurity is a complex issue. There's probably no issue that has become more crucial, more rapidly, but is less understood, than cyber security. There are many factors that influence cyber security; however, we must set expectations first. Cyber threats can be recognized and understood, detected, resolved and managed, but never completely eliminated.

The Cyber Security Conversation

Here are several points that should be part of your cyber security conversation:

- Cyber security is a disruptive trend changing the face of your business.
- The cyber threat of the day we see on the news always catches our eyes but fails to communicate the variety of vulnerabilities and threats and the harm it causes businesses.
- Cyber security is about stopping people from breaking into things. There's no such thing as absolute security, it is about making it harder for hackers to get in.
- No company is too small to face a cybersecurity attack.
- Understand that cyber security is no longer "by obscurity".
- Cyber security is an undervalued and misunderstood element to business operations.
- Cyber security should be given a more prominent role on the executive team, with more emphasis placed on avoiding the breach in the first place rather than trying to conduct damage control after the fact.
- Organizations that treat cyber security as a strategic issue perform better than those that view it as a tactical one.
- There is a direct link between security and the business value of a company.
- A negative cyber incident damages a business's reputation. A businesses reputation is a company's most valuable asset.
- Think about cyber security in terms of reducing risk and legal headaches rather than in terms of return on investment.
- Cyber security incidents are the ultimate threat to a business's brand reputation

Cyber Security Statement.

Does your company have a cyber-security statement? How about the companies in your supply chain? Do they?

When it comes to your supply chain, exercise due diligence before engaging with third party providers; include appropriate cyber protection in contracts with technology service providers; take adequate measures to verify that the third party is protecting your data and access to it adequately. However, remember, *if a problem arises, the problem is yours, even when it's your vendor's problem.*

Cyber prevention and protection is not a nice-to-have, it is a must-have.

There are two types of companies; those that know they've been breached, and those that haven't figured it out yet. Which one are you?

While we focus on revenues and profits; unfortunately, cyber security doesn't drive either of those two priorities *(Or does it?).*

Ignorance is not bliss when it comes to cyber security. The fact that you aren't seeing or hearing about potential threats by the security team shouldn't make you feel better. It should make you wonder if you aren't doing enough, or even potentially doing something wrong. Lack of information or news is about the worst possible scenario when it comes to cyber security.

Scrutiny of firm's cyber security policies is only going to increase in the future. Doing nothing is a risk.

A hacker can use any device as a jumping off point to get onto other devices and systems, introduce malware, viruses and worms, gain entry to data or engage in other detrimental activities.

Cyber risks to business are moving too fast for a purely reactive approach ---you must be proactive; cyber security should NOT be seen as an issue for the IT department alone. Companies need to know what's connected to their networks, what's running or trying to run on their networks, limit and manage those who have admin privileges.

Cyber Security and the Board Room

Cyber security is becoming a front business issue and a board room issue. After a series of high-profile data breaches and warnings, corporate boards find themselves dealing with cyber threats and security issues. Not long ago, cybersecurity was a term rarely, if ever, heard in the boardroom. Rather, information security was deemed to be a risk managed solely by the chief information or technology officer. Those days are gone. With the long list of high profile cyber security hacks—and the after effects that include drop in shareholder value, brand and customer erosion, regulatory inquiries and litigations—cybersecurity has become an increasingly challenging risk that boards must address.

According to The Wall Street Journal, so far this year, 1,517 companies traded on the New York Stock Exchange or Nasdaq Stock Market listed some version of the words cyber security, hacking, hackers, cyber-attacks or data breach as a business risk in securities filings. That is up from 1,288 in all of 2013 and 879 in 2012.

What You Can Do

Despite numerous advancements in security technology, the cyber threat landscape is growing more dangerous. You can't change the fact that cyber threats exist, but you can arm your business with the proper cyber prevention measures and reduce the risk of unauthorized system access. In order to mitigate these ever-evolving threats, you need a multi-layered, proactive security strategy.

A comprehensive cyber security program includes a defense-in-depth strategy and leverages industry standards and best practices to protect systems, devices and the networks they run on and detect potential problems along with processes to understand current threats and enable timely response and recovery. Cyber security should be an integral part of the design of your systems and the deployment, not an afterthought:

- Get the cyber security conversation started
- Treat every system and every device as critical; protect them
- Include perimeter defenses detection as well as a pre-planned response plan
- Make cyber security part of the organizational and DNA
- Build cyber security solutions and plan it into the front-end design
- Embrace a threat-centric approach to them, with solutions that work together, collecting and sharing intelligence, with a coordinated focus on threats
- Examine the use of remote connections; make sure these are secure
- Frequently monitor for vulnerabilities and have a mitigation plan in place
- Deploy a defense in depth approach; utilize multiple layers of cyber prevention
- Vet the cybersecurity defenses of those you do business with; do cybersecurity due diligence on vendors
- Limit vendors' access to their systems
- Utilize two-factor authentication
- Have a well thought-out and detailed incident response plan

Contracts with vendors should address cybersecurity by including an obligation to maintain reasonable cybersecurity, and provide notice when the vendor has a breach of their systems. There should also be a provision to audit their cyber defenses.

Inventory of all your systems and devices

For contractors doing business with organizations, make sure your internal systems are protected from cyber-attacks. You don't want to become an unwitting accomplice to criminals who compromise your systems and then ride piggy-back to your customers where they can do damage.

- Create an on-boarding process for vendors and suppliers that includes cyber security

Conclusion

Cyber security is a trade-off. We make those trade-offs on a daily basis. We make them when we decide to lock our doors in the morning, when we choose our driving route and when we decide whether we're going to pay for something with a check, credit card, or cash. We are experiencing a reality check. Today's reality is this: No matter what business you are in, no matter where in the world you are—everything on a network is at risk. One thing we can be sure of is that threats aren't going to go away. There is a pressing need for proactive cyber security vigilance. The best way to approach cyber threats is to realize it is not if an attack will happen; it is only when. Successful cyber threat prevention involves multiple paths of defense and layers of protection. It is all of our responsibility to take an active role.

About Lynxspring

Lynxspring is changing the way devices and systems communicate, collaborate and are secured across enterprises. Our technologies and solutions are enabling users to go further to manage and operate their facilities and equipment smarter, safer, more efficiently and securely, and at peak performance levels. We have changed the way control systems are built and distributed. For more information visit www.lynxspring.com

Lynxspring is the creator and developer of LYNX CyberPRO™, the industry's first cyber-threat protection solution designed specifically to enhance the protection of commercial control and energy management systems and other networked Internet of Things devices. For more information visit www.lynxcyberpro.com