SOLUTIONS & SUCCESS
The Inside Story

Implement security layers now to beat this three headed monster, an insiders guide every business owner needs to know now.

2022

www.baroan.com

Implement security layers now to beat this three headed monster, an insiders guide every business owner needs to know now.

The year 2021 will largely be remembered as the second year of the pandemic, and rightly so. COVID-19 disrupted lives and caused severe economic hardship, even going into 2022.

However, that's not the only trend worth considering in 2021.

Since the start of the pandemic, the rate of cyberattacks grew 400%—the fact is that a rising tide lifts all ships. As cybercrime becomes more prevalent, your organization becomes a more likely target, no matter its size.

The Threat Of Cybercrime Is Evolving

Every day, cybercriminals attempt to adapt their methods to overcome new standards and defenses in cybersecurity. Nowhere is this more evident than with ransomware.

Just a few years ago, ransomware wasn't as big of a concern. While high-profile incidents like the WannaCry attack on the NHS were concerning, they were far and few between. If you had a recent backup of your data in place, you could rely on that to replace your data in the event it was encrypted by ransomware.

Since then, however, the way cybercriminals use ransomware has evolved. They have improved their tactics and capabilities, allowing them to do much more damage, and demand much more money.

Characteristics of modern ransomware attacks include:

- **Expanded Timelines:** Sophisticated attackers sneak ransomware into a breached network and then lay dormant for weeks or months, ensuring their method of entry isn't discovered right away. This gives them time to embed themselves, steal data, and more, all before they actually activate the ransomware and infect the systems.

  Without undertaking extensive forensic processes, an infected business won't know how far back they need to go to back up their systems. Or, even worse, it will be so far back that they've already expunged those backups to make room for more recent versions.

- **Improved Capabilities:** Modern forms of ransomware can even target and infect backup hard drives and cloud-based data if the connections are left unsecured. That's why cybersecurity professionals are now recommending digitally-air-gapped backups as well.

Given the effectiveness of modern ransomware attacks, defensive methods and best practices from just a few years ago are already losing feasibility. All of this is to say that you can't assume you won't be infected at some point.

Failure To Comply With Data Security Laws Will Cost You

In light of the increasingly digital nature of our world, and the growing rate of cybercrime, many countries and states are rolling out new data security compliance laws. These are designed to encourage or require businesses that store private consumer data to properly protect it against theft and exposure.

- **CCPA:** The California Consumer Privacy Act *(CCPA)* took effect on January 1, 2020. This privacy act dictates consumer rights and company responsibilities in relation to collected consumer data.

  The law, AB 375, will allow any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with.

  The law also allows consumers to sue companies if the privacy guidelines are violated. It's important to note that consumers can take legal action, even if no breach has occurred.

- **GDPR:** The General Data Protection Regulation *(GDPR)* applies to organizations that conduct business in Europe to ensure the protection of confidential data for citizens in the European Union *(EU)*. This is true for companies no matter where they operate.

  If you do business with EU citizens, you must comply with the GDPR, which means that almost every major corporation and media group in the world is affected. Businesses that fail to comply could be fined 4% of their global revenue, up to $20 million.

- **NY SHIELD ACT:** New York's Stop Hacks and Improve Electronic Data Security *(SHIELD)* Act is designed to make sure that organizations do their due diligence to protect the private data they access that belongs to residents of New York state. This means implementing a range of cybersecurity safeguards, and, in the event of a failure, facing severe non-compliance fines.

  If you're not fully aware of how this compliance system works, what's expected of you, and how non-compliance is dealt with, then you're at risk of major fines —up to $250,000.

Even if these systems don't apply to you and your business, it's only a matter of time until similar legislation is enacted in your state or at the federal level. That's why you should start following an accepted cybersecurity framework sooner rather than later.

One potential framework to consider is NIST 800-171.

What Is NIST 800-171?

The National Institute of Standards and Technology *(NIST)* was founded in 1901 by Congress to remove obstacles in US manufacturing competition. It intersects with business cybersecurity when it comes to NIST Special Publication 800 - 171 "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations."

In 2016, NIST released NIST 800 - 171 to provide a cybersecurity framework that protects data not covered under a "Classified" label, but which still could prove dangerous for American interests should it be obtained by an adversary.

Although NIST *(and the related CMMC regulatory system)* are most directly implemented for manufacturing firms, that doesn't mean you can't follow its framework. The minimum cybersecurity standards are described in NIST Special Publication 800-171 and broken down into fourteen areas:

1. **Access Control:** You must limit system access to authorized users.

2. **Awareness & Training:** You are required to promote awareness of the security risks associated with users' activities, train them on applicable policies, standards and procedures, and ensure they are trained to carry out their duties.

3. **Audit & Accountability:** You must create, protect, retain and review all system logs.

4. **Configuration Management:** You are required to create baseline configurations and utilize change management processes.

5. **Identification & Authentication:** You must authenticate information systems, users, and devices.

6. **Incident Response:** You're required to develop operations to prepare for, detect, analyze, contain, recover from, and respond to incidents.

7. **Maintenance:** You must perform timely maintenance of your information systems.

8. **Media Protection:** You must protect, sanitize and destroy media containing CUI.

9. **Personnel Security:** You're required to screen individuals before authorizing their access to information systems, and ensure these systems remain secure upon the termination or transfer of individuals.

10. **Physical Protection:** You must limit physical access to and protect and monitor your physical facility and support infrastructure that houses your information systems.

11. **Risk Assessment:** You are required to assess the operational risk associated with processing, storage, and transmission of CUI.

12. **Security Assessment:** You must periodically assess, monitor and correct deficiencies and reduce or eliminate vulnerabilities in your organizational information systems.

13. **System & Communications Protections:** You must monitor, control and protect data at the boundaries of your system, employ architectural designs, software development techniques and system engineering principles that promote effective information security.

14. **Protection System & Information Integrity:** You're required to identify, report and correct information and any flaws in your information in a timely manner. You must also protect your information systems from malicious code at appropriate locations, and monitor information security alerts and advisories so you can take appropriate actions.

Cybercriminals Are Targeting Weak Links In The Supply Chain

Are you the most viable target in the supply chain?

The fact is that cybercriminals know where their efforts will be most effective. They won’t have much success targeting massive companies that have the necessary resources to defend themselves. That’s why they target smaller companies in the supply chain of those larger businesses.

Cybercriminals can take advantage of the small company's lower security standards and still access the same data. If you run a small business that shares data with larger companies, you need to consider yourself a target by proxy.

For small businesses, the situation is especially dire. According to a study conducted jointly between Cisco and the National Center for the Middle Market, over 50% of small businesses have no cybersecurity strategy or plan in place and for those that do, most have not reviewed the plan in over a year.

A cybersecurity strategy and plan, once created and adopted, must be reviewed at least annually to ensure that current threats are being included. Cybersecurity is not a one-and-done solution; the threat landscape evolves at a rapid pace and frequent reviews ensure that the plan will help reduce an organization's cyber risk profile. That's why you need to be aware of the greatest threats to your business and plan against them.

Are You Sure Your IT Company Is Keeping You Secure?

You can't assume that all IT companies deliver the same degree and quality of cybersecurity support.

You would be shocked at what the Baroan Technologies team has uncovered during our assessments of new clients' systems. Repeated passwords, unprotected endpoints, missing MFA, the list goes on.

Selecting a company to maintain your technology is one of the most important decisions you can make for your business. You must find the most competent and reliable IT support provider in your area.

Need Expert Cybersecurity Guidance?

Don't let basic cybersecurity put you at risk, and don't assume you have to handle advanced cybersecurity all on your own—Baroan Technologies can help you assess your cybersecurity and develop a plan to enhance it.

You can start improving your cybersecurity by getting in touch with our team.

Baroan TECHNOLOGIES