STL 10 Cybersecurity Best Practices

It is important to take a layered approach with your organization's security. These ten cybersecurity best practices are items you may not have considered, but definitely should.

1. Implement a Formal IS Governance Approach
Establishing and maintaining an information security framework is a great place to start. This framework is more important than every shiny tool in your security stack, as it should align your assurance strategies and support the business.
When selecting one of these methods, ensure your program provides the ability to employ a risk-based approach and enables your teams to detect incidents, investigate effectively, and respond quickly.

2. Stop Data Loss
Most enterprises rely on employee trust, but that won't stop data from leaving the company. The truth is, users steal data. A recent survey of more than 1,500 security professionals found that data exfiltration from an endpoint is the top security concern of 43% of them. Now, more than ever, it is extremely important to control access, monitor vendors and contractors as well as employees, and know what your users are doing with company data to reduce data leakage.

3. Detect Insider Threat
It's true that employees are your biggest assets, but they can also be your biggest risk. While well-trained users can be your security front line, you still need technology as your last line of defense. Monitoring user activity allows you to detect unauthorized behavior and verify user actions are not violating security policy. Insider threats may go undetected, but the fact of the matter is insider breaches are extremely costly.

4. Back Up Data
Backing up your files may seem like common sense, but any organization that has been hit with ransomware – such as Petya or Wannacry– will tell you how important it is to ensure this best practice. It is crucial for organization to have a full working back up of all of data not only from a basic security hygiene prospective, but also to combat emerging attacks.

5. Beware of Social Engineering
The technology and IT security policies you implement doesn't replace the need for common sense or eliminate human error. Social engineering tactics have been used successfully for decades to gain login information and access to encrypted files. Attempts may come from phone, email or other communications with your users. The best defense is to…

6. Educate and Train Your Users
No matter how gifted, your users will always be your weakest link when it comes to information security. That doesn't mean you can't limit the risk through regularly educating your users on cybersecurity best practices. Training should include how to: recognize a phishing email, create and maintain strong passwords, avoid dangerous applications, ensure valuable information is not taken out of the company in addition to other relevant user security risks.
In these sessions, it may feel like you are putting your people to sleep, or it might be going in one ear and out the other, but training your people on proper cyber security hygiene is critically important. Finding creative techniques to make the training stick will go a long way.

7. Outline Clear Use Policies for New Employees and 3rd Parties
To strengthen and clarify the education for cybersecurity best practices you give your users, you should clearly outline the requirements and expectations your company has in regards to IT security when you first hire them. Make sure employment contracts and SLAs have sections that clearly define these security requirements

8. Update Software and Systems
With cyber-criminals constantly inventing new techniques and looking for new vulnerabilities, an optimized security network is only optimized for so long. Even as recent as a couple months ago, organizations fell victim to a major breach with the Heartbleed vulnerability. To keep your network protected, make sure your software and hardware security is up to date with the latest and greatest.

9. Create an Incident Response Playbook
No matter how well you follow these best practices, you still may get breached. In fact, nearly half of organizations suffered a security incident in the past year. If you do, having a response plan laid out ahead of time will allow you to close any vulnerabilities, limit the damage of a breach, and allow you to remediate effectively.

10. Maintain Compliance
Hopefully these best practices are a useful guideline for keeping your business safe, but you do have another set of guidelines available to you. Regulations like HIPAA, PCI DSS and ISO offer standards for how your business should conduct its security. More than a hassle, which you need to prepare audit logs for, compliance can help guide your business.

Final Thoughts
There are countless cybersecurity best practices and strategies that should be considered, and these are just a few of the ones that we think are most important. Are there any essential best practices that we missed? Feel free to reach out to us directly on www.stlcomms.com to share your thoughts and exchange insights.