8 QUICK WINS

that will improve your cybersecurity posture without breaking your budget

Contrary to popular opinion, improving your cybersecurity posture does not have to be an expensive investment. It is possible to vastly improve enterprise protection and monitoring by taking some very basic steps that provide significant returns.

Based on our work with clients on the cyber front lines, here are 8 quick wins you can implement now that won't break your budget.

1. **Inventory your information assets.** Take a hard look at what you really know about your IT assets and how they are managed. You can't protect what you don't know you have! But you can guarantee that if your network is targeted, "Mr. Ima Blackhat" will find that unpatched system you didn't know about and exploit it. When it comes to asset inventory, deploying an automated discovery tool is an inexpensive quick win to becoming more aware of your enterprise systems. Deploy both active inventory systems (dynamic host configuration protocol/DHCP server logging and network address scanning tools) and passive inventory systems (which analyze network traffic to discover hosts).

2. **Assess your endpoint protection profile.** So, now you know what you have. You've attained "network enlightenment." But how do you manage operating system (OS) patches to these systems (i.e. laptop and mobile device updates)? Are you ensuring that every endpoint that touches your network is securely configured? Here again, automation is your friend. Deploy automated patching tools that will deliver the latest OS updates to your endpoints after they've been thoroughly tested and vetted to play nice in your environment.

3. **Review physical access security.** Cybersecurity is about protecting your most crucial business assets: your data and its supporting infrastructure. Simply stated, lapses in physical security may lead to unauthorized access to systems and data (and, of course, access to secure places). Make sure you shore up any physical security gaps, which will help secure your technology infrastructure as well. Verify that those who have access to data and infrastructure really require that access. Also look for holes in existing processes such as employee termination procedures to identify and remove access for those who no longer require it.

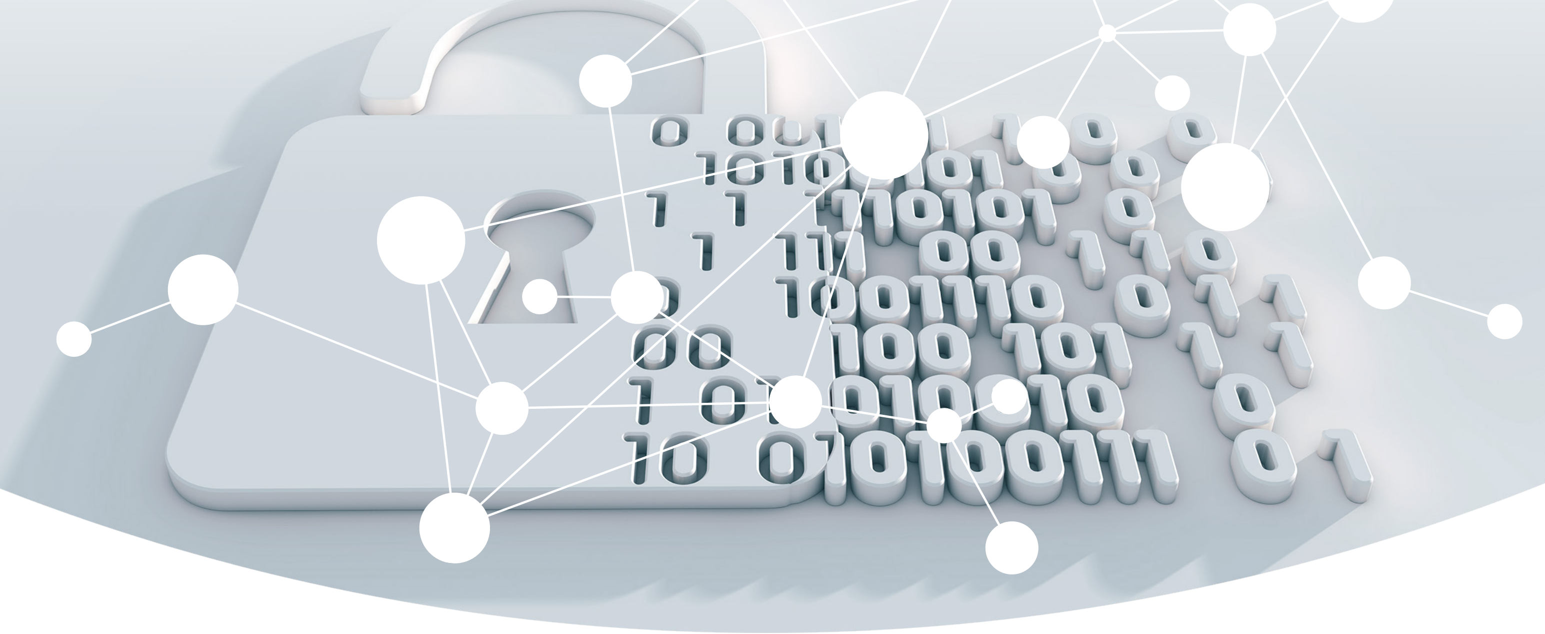
4. **Explicitly address mobile devices.** More and more mobile devices are connecting to business networks. Embracing the bring your own device (BYOD) movement is all the rage now. However, regardless of whether a device is business or personal, there's a limit to controlling what it can do with your data once you grant access. Make sure you have a clear understanding of the applications and data being accessed by mobile devices in your enterprise by employing a mobile device management solution. If you aren't being explicit about the apps and connections you believe are appropriate for these devices, your employees can't be expected to make safe choices.

5. **Evaluate your existing tools.** Do you have network monitors? Do you have log aggregation tools? Can you get more out of some of these tools? Implementing additional features of your existing security tools could possibly save you a ton of money and time. Work with what you have before investing in new solutions—you may be able to augment inexpensively to fill security gaps.

6. **Focus logging activity on mission-critical systems.** Compare anomalies against access requirements. Be careful to turn on logging with an understanding of how systems work together. Resist the temptation to turn on every monitor available in your infrastructure as it will complicate root cause analysis and overwhelm your resources.

7. **Continually educate employees.** Training encourages proper behavior and serves as a constant reminder to help engrain cybersecurity awareness into your organizational culture. Embodying a security culture is one of the best ways to improve your security posture. Your employees are the first line of defense and usually the first avenue of attack. Engage them with shorter training segments in a more frequent manner. In other words, have them learn a focused topic for 10 to 15 minutes every quarter, instead of the 1 to 2 hour drudgery typical of annual security training.

8. **Seek employee input.** Cybersecurity is a business problem, and IT management is about empowering your resources and listening to those who know your business. Your employees are the best source of information, and sometimes the simplest changes to policies and procedures can have the greatest impact. Ask them to align your identified risks with the mission of the organization, and roadmap your improvements based on input from the business.



CGI

Experience the commitment®

Contact us at info@cgi.com
or visit www.cgi.com/cyber