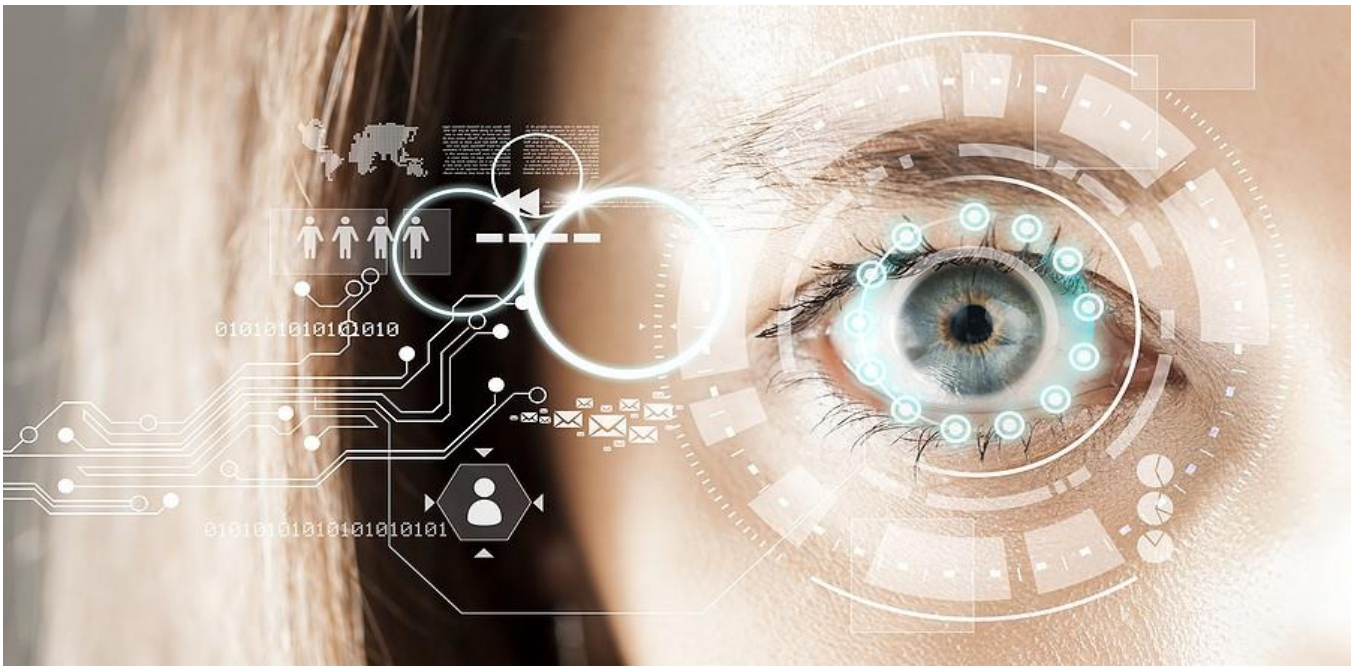
Move Beyond Compliance Checkbox Cybersecurity to Comprehensive Strategy



In recent years, privacy regulations have shaped cybersecurity strategy for many organizations. Audit checklist in hand, administrators develop policies and training plans, review workflows and implement technologies that promise compliance. After a successful audit, they breathe a sigh of relief. But compliance checkbox cybersecurity does not provide adequate protection.

When organizations focus their efforts instead on securing data rather than checking boxes, they begin to see the real benefits. The chance of a breach diminishes. And when security incidents do occur, the companies detect and contain them early, minimizing the damage. Equally as important, this proactive approach supports innovation and inspires customer loyalty.

Why Compliance Checkbox Cybersecurity Falls Short

Privacy regulations typically mandate the minimum set of controls required to protect against known dangers. But dangers evolve quickly, as bad actors continually hone their methods and develop new weapons. What provided sufficient protection against last year's threats will not provide adequate security now.

Just as the threats evolve on a continual basis, the attack surface also broadens. Companies add employees, vendor relationships, equipment, and software. Workflows change. A focus on compliance can mean that the organization addresses security on an annual basis. In reality, effective cybersecurity requires continual monitoring and a comprehensive approach.

Top to Bottom Cybersecurity Awareness

Privacy regulations often require that organizations deliver security awareness training. However, effective security education involves more than an annual event. When organizations realize that employees play a pivotal role in information security, they work to build a culture of security awareness.

All personnel who deal with information need to understand cyber risks and their role in protecting vital information assets and privacy. From the c-suite to the interns, employees should know security best practices, as well as job-specific policies. This will require repeated training events and reminders.

Address Supply Chain Vulnerabilities

In addition to educating employees, companies must also look at their vendors. Increasingly, cyber criminals exploit supply chain vulnerabilities to infiltrate larger organizations. For instance, in the NotPetya attack, hackers targeted an accounting software vendor. Then they used the auto update feature to install infected code into the systems of multiple companies.

To help mitigate the risk of a similar scenario, organizations first need to build a list of all third parties with access to the system. They should specify compliance standards that the vendors must meet and monitor that compliance. Monitoring should include reviewing logs of vendor access on a regular basis.

Disaster Plan

Even with a solid cybersecurity controls in place, security incidents will occur. A comprehensive information security strategy must also include an incident response plan. Begin with 24/7/365 monitoring to reduce response time and improve the likelihood of a successful recovery.

Then define an incident response team and communication plan before a breach occurs. Make sure that all key players know their roles and responsibilities. Then, when an incident does occur, they have the playbook and can act immediately.

Partner with Security Experts

For small to midsize businesses, the task of implementing an effective cybersecurity infrastructure can stretch the limits of in-house expertise and budgets. In these cases, partnering with information security experts will fill critical gaps.

A quality security provider stays up to date with emerging threats, as well as with current cybersecurity best practices. They can help organizations implement security controls properly, providing optimal security. And they can provide the continuous monitoring essential to maintaining a strong security posture.

For over two decades, eMazzanti has delivered scalable, cost-effective cybersecurity services. We will start with a cybersecurity assessment and help you tailor a strategy geared to your specific environment and needs.