Business Cyber Security Resolutions for 2023 Focus on Smart Investment

In this year's Allianz Risk Barometer, from global insurance giant AGCS, cyber incidents ranked as the number one business risk of 2022. At the same time, rising costs have businesses watching budgets closely. Thus, as organizations make their business cyber security resolutions for the coming year, they will focus on areas that give substantial ROI.

For many organizations this will mean prioritizing basic cyber security best practices or capitalizing on automation opportunities. Others will strengthen the first line of defense by increasing cyber security awareness. And as cloud migrations and connected devices broaden the attack surface exponentially, adjusting security strategies in those areas proves critical.

Recommit to Making Cyber Security Basics a Priority

As a possible recession looms and budgets tighten, security leaders face increased pressure to find efficiencies. Because recessions also historically bring an increase in cybercrime, business leaders must stay focused on security. One way to strengthen security without huge expense involves prioritizing tried and true cyber security best practices. For instance:

- Update password policies – Review your current password policy and automate enforcement wherever possible. For instance, password settings in Windows can be defined to enforce a minimum password length and other complexity requirements.

- Regularly deactivate orphaned user accounts – Be sure to deactivate user accounts once employees leave the organization. Left in place, these orphaned accounts leave a door wide open for disgruntled ex-employees or hackers. Likewise revoke permissions for privileged accounts once they are no longer needed.
- Review and update backup policies – With data distributed across on-premises, cloud and remote locations, your backups may need some adjusting. A cloud backup solution can provide critical connectivity across all your data sources.

Automation Levels the Playing Field

In addition to cyber security basics, automation offers another opportunity for great ROI. Automating security processes not only frees up existing staff but also helps to level the playing field in a battle against highly automated attacks. And it decreases response time and reduces the chance for human error.

Start by automating patch management. The average organization has hundreds of devices, systems, and software applications. Staying on top of security patches and updates manually can eat up valuable time but leaving systems unpatched introduces unacceptable risk. An automated system will drastically reduce time spent identifying risks and deploying patches.

Additionally, automated scanning, particularly when combined with machine learning, can detect and even remediate vulnerabilities that hackers could exploit. And automated log analysis can identify suspicious traffic on the system, allowing security teams to catch infections early.

Adjust Security Strategy to Protect Data in the Cloud

As more workloads move to the cloud, companies need to ensure that security practices match the data landscape. Traditional on-premises security strategies will not effectively address the additional risks that come with cloud computing.

The cloud environment necessitates a robust, multi-layered approach to cloud security. This includes strong encryption, as well as endpoint protection and particular attention to identity and access management. Additionally, a cloud access security broker (CASB) will act as a firewall in the cloud, using automation to detect and address risky behavior.

Increase Cyber Security Awareness

Approximately 90 percent of data breaches happen because of a phishing attack. That makes employees both the weakest link and a key line of defense. And it means that wise organizations invest in creating cyber security awareness among employees at all levels. Start by training users to recognize and appropriately respond to phishing attempts.

Close Back Doors by Strengthening IoT Security

Gartner predicts that in 2023 the number of IoT-connected devices will rise to 43 billion. Because they often do not actually store data, these devices tend to fly under the security radar. However, attackers can use them as gateways to gain access to the network.

This year, commit to updating your inventory of IoT devices, from routers to sensors and point of sale devices. Be sure to change default passwords for the devices and to include them in your patch management programs.

Additionally, even though IoT devices do not always store data, they gather large quantities of data. Studies indicate that 98 percent of IoT traffic remains unencrypted. Implementing encryption on these devices closes security gaps.

Jump Start Your Business Cyber Security Resolutions with eMazzanti

The security experts at eMazzanti Technologies know the threats you face, and they understand the challenge of balancing dwindling budgets and ever-increasing cyber risks. Beginning with a risk assessment, they will help you identify security gaps and design a strategy around your needs and budget.