one brightly cyber

WE MAKE CYBER SIMPLE

WHAT'S NEXT FOR 2023?

The new year is almost here. With it comes a renewed increase in cybercrime.

Cybercriminals are constantly working to find new ways to fool us and to get past our defenses.

Reports from Gartner and Verizon indicate specific areas of focus for cybercriminals going into 2023. While Gartner and Verizon are reputable organizations, take these predictions with a grain of salt because cybercriminals adapt their methods to get past our defenses, technical and human.

Digital supply chain acceptance is growing. With any new technology or technology approach comes new avenues of attack. Gartner predicts attacks on software supply chains will grow to impact 45% of companies using them by 2025.

That is a staggering number. The newness of digital supply chains means the vulnerabilities are still to be discovered. Similar to the risks experienced in the rapid movement to the cloud spurred by the pandemic, configuration errors will present open doors to cybercriminals. When beginning your transition to a digital supply chain be sure to get assistance from people experienced in the field. It is not the time for coming up the learning curve. The risks are too high. Remember that security includes people, processes, and premises, in addition to technology. Omitting any one of them leaves you vulnerable.

Mobile phones are the platform of choice for many people and the acceptance of personal devices for use in the business multiplies the avenues for attack. So, it is not surprising that the Verizon Mobile Security Index identifies mobile device attacks increasing by 22% in 2022 and expecting that growth to continue in 2023.

The mobile devices present so many avenues of attack, the devices themselves, apps both personal and business, the platforms accessed by the apps and by the devices, and maybe most importantly, the fact that mobile devices have been used in Multi-Factor Authentication. SMS based Multi-Factor Authentication is far too easy to compromise giving cybercriminals access to company accounts, applications, servers, and more.

Be sure to use MFA, but sure it is a phishing resistant form of MFA. Authenticator apps are a recommended approach. See our Insight on MFA for more information on this.

The Global Risks Report from the World Economic Forum says that despite improvements in technology, 95% of cybersecurity incidents are attributable to people. This means people continue to be the weak link in the cybersecurity chain. Certainly, use good protective technology and follow best practices.

But most importantly, educate your users at every level up to and including executives. Use surprise tests to see who still takes the bait.

WE MAKE CYBER SIMPLE

WHAT'S NEXT FOR 2023?

Data privacy is a driving force in legislative action. The European Union implemented GDPR, General Data Protection Regulation, a few years ago. It was very clear that each person owned all data about them and companies or organizations could not collect it, store it, use it, sell it, or trade it without explicit permission from the user.

The ground swell for data protection laws in America is growing with some states implementing laws already. This will lead to pressure for the federal government to take this up so that companies or organizations don't have to try to comply with different laws in different states.

The first step on this path, and one you can take now, is to begin to inventory the data you collect, why you collect it, every place it is stored, what it is used for, what you do with it, and how you dispose of it. Without this it will be impossible to comply with any data protection laws. And the laws are coming.

Begin now and good luck in 2023.

Are you ready to get serious about protecting your assets and your company? Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.