DS24
DataSure Twenty Four
Your Cybersecurity Partner

DataSure24's December Brainbytes: The More Things Change...

DataSure24 is your cybersecurity partner, working to help meet your company's specific security needs. Each month, we'll offer bytes of information about emerging risks, news, and protective measures to help keep your data safe and your network secure.

After high-profile data breaches at Google, Twitter, Uber, LinkedIn, and Rockstar Games, it seems like no company is immune to cybersecurity attacks. They've become an unfortunate part of the business world, with financial losses from cybercrime exceeding the total losses incurred from the global trade of all illegal drugs.

As we see advancements in technology, cybersecurity also evolves and matures in its ability to take down cyber threats and attacks. That said, companies are increasingly spending their IT budgets on security, whether it's hardware, software, cloud-based or other managed services.

With the world in constant flux, it's difficult to know exactly what will happen in 2023. However, we believe that cybersecurity will be increasingly driven by:

- Compliance
- Insurance
- Remote and Hybrid Workplaces
- Cloud Computing
- Artificial Intelligence
- Insider Threats

Compliance

In order to ensure the protection of customer information, several industries are facing stricter requirements related to cybersecurity.

- Financial institutions like mortgage lenders, debt collection agencies, and car dealerships, must comply with updates to the FTC Safeguards Rule by June 9, 2023.
- Defense contractors and subcontractors must obtain CMMC certification by 2026.
- The DFS is in the process of approving amendments to the NYDFS Cybersecurity Regulation (23 NYCRR 500) affecting banking, insurance, financial services and other covered institutions.

Meeting compliance requirements is now a part of business operations, and it's likely that sectors and institutions not affected by those listed above will face their own changing regulations in the near future.

Remote and Hybrid Workplace

On a global-scale, gaps in security cost businesses trillions of dollars in losses each year. And with companies shifting to remote work since the beginning of the pandemic, they have only become more vulnerable to attacks from hackers.

According to IBM's Cost of Data Breaches Report 2022 the national average cost of a data breach is $9.44 million (whether ransomware was involved or not). In the healthcare industry, the recovery cost was approximately $10 million. In cases where remote working was a factor in the breach, the average cost increased by around $1 million.

According to the Forbes Technology Council, the shift to remote and hybrid work has created changes in security and privacy that will require companies to prepare for the long-game in regard to developing and implementing cybersecurity plans that factor all of these changes.

Cloud Computing:

In response to a shift to remote and hybrid workplaces and increased cybersecurity attacks, more and more organizations are moving toward cloud storage in efforts reduce vulnerability and mitigate attacks.

In using this new model, companies will begin to, or further implement security measures, including:

- Zero Trust
- Multi-Factor Authentication (MFA)
- Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication, Reporting and Conformance (SPF, DKIM and DMARC)
- Hardening Guides

While cloud storage has many positives, including speed, cost-effectiveness, and unlimited storage capacity, it should not be viewed as the end all be all solution to cybersecurity. The network will be only as secure as you make it, by ensuring good policies and procedures are in place. It's encouraged to bring an expert in who can look at the settings and determine which ones are the most secure.

Policies and procedures, then, must be consistently monitored and updated to ensure data is protected from leaks.

Artificial Intelligence (AI)

People store a wide range of information and complete thousands of small tasks each day, leaving a large margin of error for faulty decision making. Machines, however, are able to store seemingly endless amounts of information and target a specific number of tasks without deviation.

According to the Forbes Technology Council, in addition to making cybersecurity less expensive, AI will be more efficient, using a large dataset from potential cyberattack scenarios to help identify attacks and analyze threat patterns. This not only helps to prevent similar attacks in the future, it reduces the amount of time needed for cybersecurity professionals to perform routine tasks.

While further implementation and dependence on AI offers a slew of benefits, this tool does not signal the end of a human role in cybersecurity programming. It must be seen as a tool that, with correct oversight, has the potential to make systems more efficient. The analysis is only as good as the data the software is using. Garbage in, garbage out.

Insurance

Companies will have to have true security plans, demonstrating increased controls and compliance with regulatory requirements, in place in order to secure coverage. This will be key to insurers better supporting their customers and more accurately pricing cyber risk.

Insider Threats

Human error is still one of the primary reasons for data breaches. According to a study by IBM, 95% of total cybersecurity breaches were indirectly the result of an employee action. Even more, insider threats saw a greater emergence in 2022, making it even more important to ensure staff are regularly educated on cybersecurity issues, to help safeguard data in every way possible.

Employees with a lack of, or poor, cybersecurity awareness can cost you more in the long run. As mentioned above, the average cost of a data breach in the United States is $9.44 million.

The more things change, the more they stay the same.

Many cybersecurity trends have been predicted for 2023. Despite increased global stability, however, the world is still changing rapidly. At the end of the day, it all comes back to good cybersecurity.

Cybersecurity should always be a business priority. ***Unprepared organizations will become easy targets for cyberattacks.*** *Now is the time to learn the potential cybersecurity risks for your business, and build a complete cybersecurity plan.*

For more info on making a plan, check out our latest blog: The More They Stay the Same

If you would like to speak more about how DataSure24 might help your company meet its security needs, contact us by clicking below, or call (716) 600-3724. We look forward to hearing from you!

Email Us!

DataSure24, 350 Main Street, Suite 550, Buffalo, NY 14202, 716.600.DS24