GBS

AMERICA'S PRODUCTIVITY PARTNER

Data Hacks and Breaches 101

Understanding and Recognizing Threats and Protecting Your Data from Cybercriminals

Managed Technology Solutions

Overview

Data security, cyberattacks and data breaches are among the biggest and most serious challenges facing businesses today. The ability of companies to keep their customers' data from falling into the hands of thieves is imperative for long-term survival and success in the marketplace. Sensitive, private and personal data—including credit card and social security numbers, email addresses, usernames, passwords, phone numbers and buying histories and patterns—can be readily available to hackers that gain unauthorized access to a company's network. Essentially, hackers will look for any business or personal data that can be sold and used to breach financial accounts, steal a person's identity or make fraudulent purchases and transactions.

GBS assists organizations with eliminating these critical challenges and threats by customizing Managed Technology Solutions that provide robust protection against dangerous hackers and breaches. We understand how the safety and security of your data supports the success of your business—which is why our solutions are designed to safeguard your valuable data 24/7/365.

Challenges

Nothing provides a greater threat to data security today than cyberattacks, where hackers use sophisticated methods and technologies to compromise all types of digital devices, including smartphones, tablets, individual computers and entire computer networks. If and when an attack succeeds, valuable data is breached and becomes available to the hackers.

According to the Pew Research Center, nearly two-thirds (64%) of all Americans have had their online data and information compromised via a major data breach, and have been impacted in at least one of the following ways:

- **41%** encountered fraudulent charges on their credit cards
- **35%** received notices that sensitive information (ex. account numbers) had been compromised
- **16%** said that someone had taken over their email accounts
- **15%** received notices that their Social Security number had been compromised
- **14%** said that someone had attempted to take out loans or lines of credit in their name
- **13%** said someone had taken over one of their social media accounts
- **6%** said that someone has impersonated them in order to file fraudulent tax returns

In addition, the Identity Theft Resource Center (ITRC) reports that 1,632 data breaches were reported and tracked in 2017, leading to approximately 198 million records being exposed. In 2018, the total number of breaches actually fell to 1,244, but it's estimated that more than 447 million consumer records were compromised. Businesses suffered the most breaches by industry, with a total of 571 (46% of the total number of breaches), while the healthcare industry fell victim to 363 breaches (29%).

"Businesses suffered the most breaches by industry, with a total of 571—46% of the total number of breaches."

Strategies

There are some simple, basic steps that everyone can take to help protect their online devices, systems and personal data. Ongoing education on the latest threats, good common sense and the use of industry best practices are all great places to start.

1. **Create unique usernames and passwords for your accounts**. Adding numbers and symbols to your login credentials makes them more difficult to guess or duplicate. Make sure your system has medium to high complexity enabled for your password strength settings, and avoid using anything associated with your identity as part of your password.
2. **Avoid using the same password or group of passwords for your accounts.** Each online site you sign into should have its own combination of letters, numbers and symbols that are used only for that particular account.
3. **Keep all of your software current by promptly installing updates when they're released.** Updates not only improve the performance of your devices and systems, but often contain the latest security enhancements and protection for their security. Whenever and wherever possible, subscribe to a managed service via an IT provider such as GBS, which manages operating system and specific application security patches on your system.
4. **Make sure your data is backed up at the end of each day.** This is "Computer 101," and could make all the difference in the world should your data or network become compromised. Most system recovery efforts from a virus situation start with the "last known good backup." Also be aware if the data on an individual PC's local drives (C: drives) is included in whatever backup process might be running on a regular basis. It is possible that the only user data files being backed up are those being saved to a network/shared drive.
5. **Use multiple, cloud-based systems to securely store your backups.** Cloud backups utilize multiple servers spread over various locations, and provide a much greater level of security than a single, in-house server.
6. **Use good judgment and don't be click happy.** If an email looks suspicious or is from an unknown source, don't open it. If a website looks questionable, don't visit it or provide any of your information. If it looks and feels like a scam, assume that it is and avoid it. It is better to have someone call you directly on an email you may have ignored, or intentionally bypassed because it appeared suspicious, than to open it and be at risk. This is particularly true for emails with attachments. Please note that system intrusion methods utilize some level of intelligence and will send you invasive emails based on websites you may have visited or used in the past—making it appear as if it's something you are waiting for or something that may pique your interest.

Solutions

In addition to the steps already mentioned, GBS offers a wide variety of products and services to take your online security to the next level. Our Managed Technology Solutions addresses security issues from multiple angles and levels, and provide businesses and individual users the most advanced protection in the industry. Our solutions include, but are not limited to:

- **Data Protection.** We offer customers data protection by automatically backing up important files in the cloud to a secure data center via the internet, eliminating the risk of losing critical information to faulty backup tapes and making it easier to restore lost data.
- **Disaster Recovery Services.** Disaster data recovery services protect your systems from occurrences such as natural disasters, fire, power failure, terrorist attacks, thefts, cyberattacks and even human error. Effective disaster data recovery services are complex, but GBS technicians are skilled at recognizing a company's needs to customize a plan that minimizes downtime and restores all data and systems. This may even include—if something qualifies as a "mission critical" component—working to establish a plan for full or partial system and/or application replication. In the case of a severe outage or some degree of a disaster, the client's main system can be restored online by accessing an alternate connection or data center location.
- **ProActive IT Support Services.** GBS offers a team of enterprise and network professionals who know computers, networks and servers inside and out to proactively take control of your system management and IT support services. This prevents potential problems from happening before they do, and insures that key hardware, software and network components always remain in good working order.
- **Security and Network Access Control.** GBS has numerous partnerships that enable us to protect a company's network from unauthorized access, non-compliance with business security policies, theft and corruption. GBS has vast experience installing firewalls, intrusion detection systems and Virtual Private Networks (VPNs) and has partnered with leading security vendors such as Cisco, Computer Associates, McAfee, Symantec, Trend Micro and more. We have also established vendor partnerships that allow us to perform operational and technical system security risk assessments. These assessments will help keep your IT-based policies and procedures up to date and identify any lingering vulnerabilities and corrective action steps that may be needed.
- **Server, Storage and Lifecycle Management.** GBS customizes affordable computer lifecycle management plans that will save your company money and energy while increasing computer and employee productivity. GBS makes it fast and simple to manage multi-vendor, multi-platform data storage and anticipates future storage needs so that capacity adjustments are easy, quick and economical. We also assess your current server situation and reorganize it for increased productivity. This is done through server consolidation and virtualization, which allows data from multiple servers to be accessed from one location.
- **Software Licensing.** As an authorized source for popular software publishers such as Microsoft and Adobe, GBS understands what each publisher requires for software licensing. We can help an organization quickly and easily manage the entire process, including contract negotiation and renewals, procurement, deployment and upgrades.

It's important to remember that effectively protecting your online devices and data is a dynamic, never-ending process that requires constant attention. Let the security experts at GBS take care of these activities for you so you don't have to.

Spend your time managing your business, not managing your online security!
Contact us today at 330.497.6728 or at richardl@gbscorp.com.