infosecfuture

NO MATTER THEIR SIZE, HOSPITALS MUST TAKE THEIR PATIENT'S DATA SECURITY SERIOUSLY

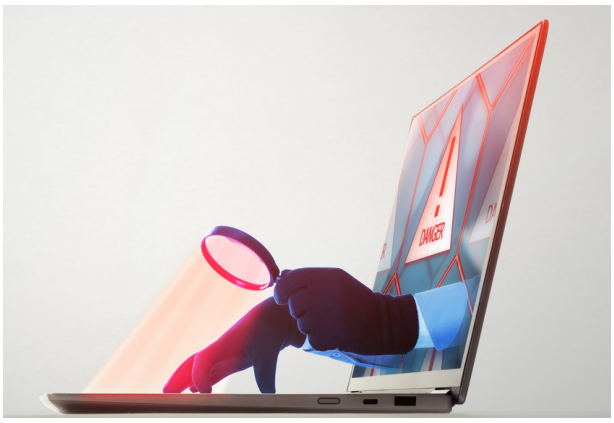
ABSTRACT

As the healthcare sector continues to offer life-critical services while working to improve treatment and patient care with new technologies, criminals and cyber threat actors look to exploit the vulnerabilities that are coupled with severe attacks. Though these prominent cyber incidents have triggered several cybersecurity initiatives, policymakers have paid relatively little attention to the considerable potential cyber risks in the healthcare sector. The Internet of Medical Things, Smart Devices, Information Systems, and Cloud Services have caused a virtual transformation of the healthcare enterprise. Digital healthcare offerings have paved the manner for simpler and greater on hand treatment, as a consequence making our lives a long way greater comfortable. However, the current healthcare enterprise has additionally turn out to be the principle sufferer of outside in addition to inner attacks. Data breaches aren't only a subject and hassle for protection experts; in addition they have an effect on clients, stakeholders, organizations, and businesses. Though the statistics breaches are of various types, their effect is sort of usually the same. In order to tackle this huge problem and stop more medical devices from being hacked, medical device assessment and penetration testing services are needed for hospital equipment and embedded devices. It's also important that healthcare organizations are aware of the negative impacts of connectivity so that they can design security measures in their systems right from the outset. Most data breaches are attributed to hacking or malware attacks. The effects brought on by a data breach can come in the form of damage to the target company's reputation due to a perceived 'betrayal of trust.' Victims and their customers may also suffer financial losses should related records be part of the information stolen.

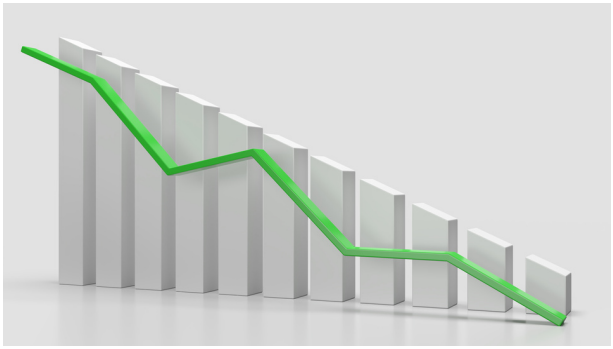
CASESTUDY

One of our client data is breached in health care sector. An independent cyber security researcher reported to the administration that a server containing users Email, Name, Address, Age, Phone Number, Chat logs, user's parent's data and staff chats were lying unsecured and open to anyone to see, copy or download.

Hospital collects user's data. This data is used to verify for registration and authentication on their portal. Such data are stored either on the administration server or a third-party cloud service provider which manages the data of the company. Sadly, it's often human error that allows attackers access to encrypted channels and sensitive information. Sure, an attacker can leverage gifts such as zero-day vulnerabilities to break into a system, but in most cases, their success involves provoking or capitalizing on human error. In my client health organisation hackers abused a third-party application that they used to provide guest services. The attackers gained access to patient records. These records included personal data, contact information, gender, account details, disease details, and medical preferences. Our client security team noticed suspicious activity and sealed the insider-caused security breach at the end of the day. This major data breach presumably affected almost twenty thousand patients data.



After the incident, my client hospital reputation has been damaged. The hospital stopped the services of its new advanced technologies to update security protocols and educate employees on social engineering attacks. The threat examples in one of our client hospital we've analyzed above occurred because cybersecurity systems didn't detect a breach and didn't alert security officers before real damage was done or because poor access management allowed for unauthorized access.



We've compiled many data breach statistics for advanced threats that also cover types of data breaches, industry-specific stats, risks, costs, as well as data breach defense and prevention resources. Hopefully, this will help organizations understand the importance of data security and how to better allocate their security budgets. To prevent such an data breaches which has happened to my client all you need is, with the correct professionals in charge of securing your data and the relevant and robust processes and procedures in place to prevent user error, then mistakes and errors can be kept to a minimum and kept to those areas where they are less likely to lead to a major data breach.

In my client organisation this data breach happened when data is accessed, modified, or deleted without authorization. Security weaknesses can lead to incidents ranging from an accidental data leak to a malicious database breach – and the effects can be devastating. Conversely, an accidental insider is someone who unintentionally causes a cybersecurity breach, such as falling victim to a phishing attack, using an unauthorized personal device, or through poor password management. Employees who have not had basic cybersecurity training are a vulnerability to their employer. When an organization becomes aware of a possible breach, it's understandable to want to fix it immediately. However, without taking the proper steps and involving the right people, you could inadvertently destroy valuable clients data used by investigators to determine how and when the breach occurred, and what to recommend in order to properly secure the network against the current attack or similar future attacks. After the cause of the breach has been identified and eradicated, you need to ensure all systems have been hardened, patched, replaced, and tested before you consider re-introducing the previously compromised systems back into your production environment.

Although a data breach can be the result of an innocent mistake, real damage is possible if the person with unauthorized access steals and sells Personally Identifiable Information (PII) or corporate intellectual data for financial gain or to cause harm.

Malicious criminals tend to follow a basic pattern: targeting an organization for a breach takes planning. They research their victims to learn where the vulnerabilities are, such as missing or failed updates and employee susceptibility to phishing campaigns.

Once inside, malicious criminals have the freedom to search for the data they want and lots of time to do it, as the average breach takes more than five months to detect.

As the relationships between consumers, organizations, governments, and other entities become ever more connected, there is a tendency for consumers to become more aware of the importance and value of personal information, as well as more concerned about how these data are used by public or private entities. Despite all efforts made by regulatory agencies and organizations to establish investments and proper protection of their operations and information , cases of data leak in large institutions are becoming more frequent and involving higher volumes of data each time.

The recent trend toward digitalization of healthcare records, increased sharing of electronic protected health information (ePHI), and new attempts by government agencies to centralize healthcare records and secure against attempted healthcare security breaches almost guarantee that the healthcare industry will see an increase in the number of, and the sophistication involved with, attempted cyber-attacks on this data. The speedy improvement of medical era and the sheer significance of the healthcare enterprise create a virtual wild west for hackers trying to capitalize from facts maliciously seized thru the loopholes they exploit. Cyber-hackers are looking at the healthcare industry and considering healthcare organizations an easy target, especially when compared to the banking, industrial, and retail sectors, healthcare historically investing less in the security of their IT, and as the value of individual's private health records on the darknet continues to increase, even the largest companies in the healthcare industry have fallen victim to data breaches.

As a healthcare security enterprise, people are trusting us with their most personal information. Therefore, it's of paramount importance to us to protect PHI / PII and ensure that we continue to live up to that trust vested in us SAFE Enterprise goes a long way in helping us do that through its quantified, trending view of breach likelihood of my critical assets and its rigorous compliance management. Securing patient, customer and organizational data is one of the top priorities for healthcare organisations. In addition to the high price offered for patient records in underground marketplaces, the rapidly increasing attack surface provides a great impetus for threat actors to attack the healthcare industry. Identity theft is a major threat to data breach victims. Data leaks can reveal everything from social security numbers to banking information. Once a criminal has these details, they can engage in all types of fraud under your name. Theft of your identity can ruin your credit, you with legal issues, and it is difficult to fight back against.

It shouldn't be a surprise that criminal hacking is the top cause of data breaches, because it's often necessary to conduct specific attacks. Malware and SQL injection, for example, are usually only possible if a criminal hacks into an organisation's system. What might come as a surprise is how many activities criminal hacking encompasses. It's usually associated with computer coding, but found that the most common criminal hacking technique involved stolen credentials. This doesn't require any technical knowledge. Crooks can purchase the credentials on the dark web, find them written down, crack them using a password-generating machine or guess them. Once a cyber criminal has a user's login credentials, they can perform any number of nefarious activities, but it usually boils down to extracting information to commit fraud or sell on the dark web, or to launch further attacks, such as phishing scams.

The most effective way to safeguard your business is to follow best practices and use a wide range of security tools to build multiple layers of protection. Infosec offers cybersecurity solutions that defend your business against data breaches using a combination of next-gen endpoint protection and cloud-based network security solutions. Keep your data in the right hands.

As external threat actors who use ransomware, phishing and other attack vectors continue to evolve their capabilities, so, too, must IT cybersecurity and data protection professionals continually up their game. A ransomware attack that prevents access to IT systems and data can shut down an organization. Organizations with multiple data centres must be able to justify the overhead expense associated with these facilities. Cloud storage can save money by reducing the need for physical footprints, but your organization must assure security and data protection. From a threat perspective, however, more data points mean increased access points for threat actors.

Security breaches committed against you or an organization with access to your personal information are serious crimes and are understandably stressful to the victims. Security breaches can result in identity theft, fraud, unauthorized accessing of your medical and financial history, or damage to your credit. However, a security breach does not ensure that you will be a victim and, luckily, there are many ways to resolve any threats to your personal information. The first step is to identify, the type of attack that occurred and which aspects of your personal information were potentially affected.

If, for instance, the theft was to a company's point-of-sale system your payment information would be at risk. If a security breach obtained access to personal identification information, such as accessing your SSN or driver's license number, you could be the potential victim of identity theft.

You can't afford to be unprepared for a data breach's aftermath. Even organizations with the strictest data security and IT policies could easily go the way of recent victims. It's up to you to control the situation and protect your brand in the wake of a data breach's potentially devastating hold on reputation .A well-executed incident response plan can minimize breach impact, reduce fines, decrease negative press, and help you get back to business more quickly. In an ideal world, you should already have an incident response plan prepared and employees trained to quickly deal with a data breach situation.

Infosec helps clients close security and compliance gaps to avoid data breaches. Our forensic, penetration testing, and audit teams identify best security practices and simplify compliance mandates (PCI DSS, HIPAA, HITRUST, GDPR). As an Approved Scanning Vendor, Qualified Security Assessor, Certified Forensic Investigator, we have tested over many systems for security.

END

infosecfuture

Reinventing Cyber Security

For over 5+ years, We are a community of cybersecurity experts that aim to make a difference in society by delivering high-quality, cost-effective, and reliable solutions to the customers we serve thereby empowering their digital journey.

We professionals at Infosec Future believe in strong digital defenses against cybersecurity incidents that are designed to disrupt organization's ecosystem.