EKRAN

Healthcare Data Security: How to Protect Patient Health Information?

www.bakotech.at

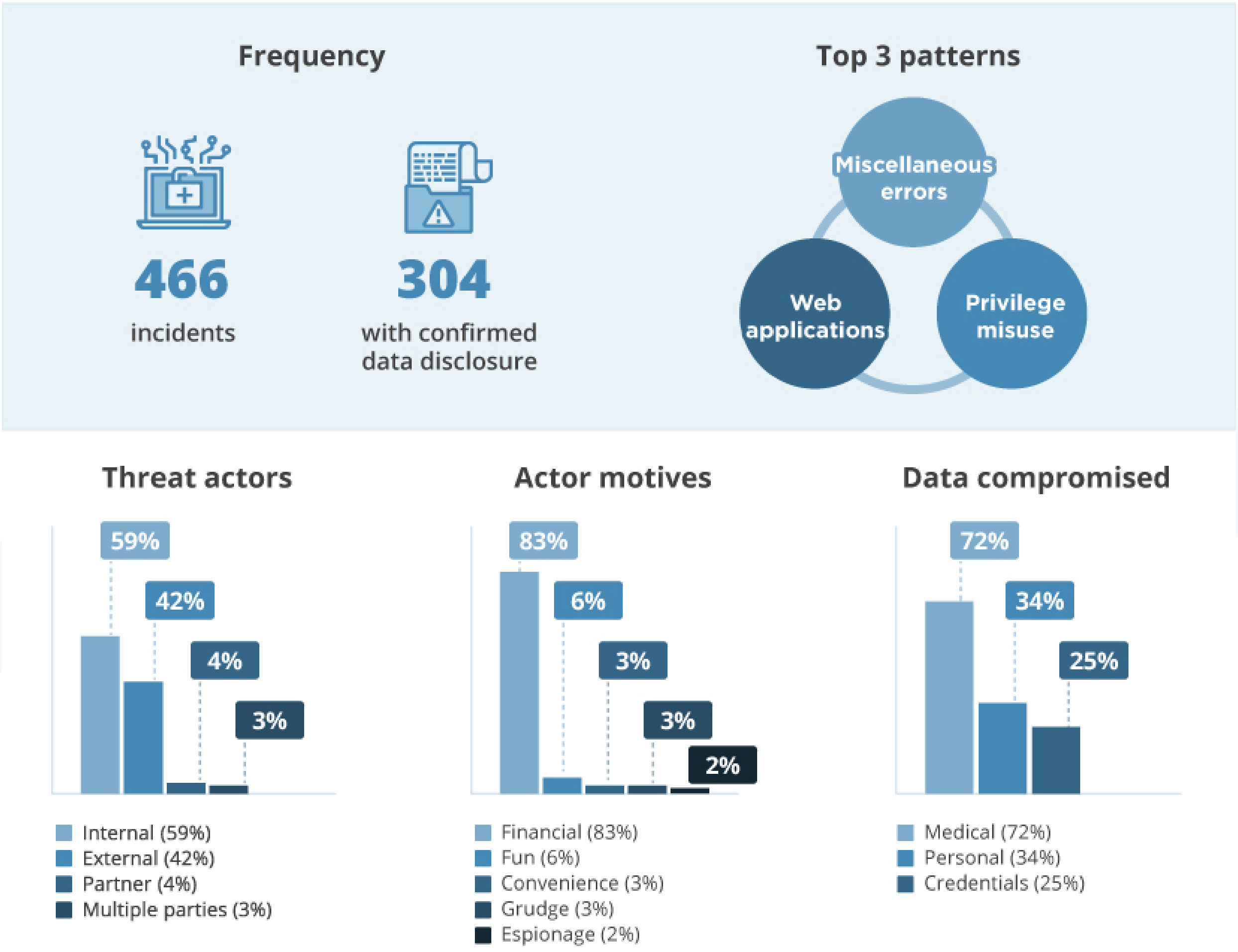
Healthcare data breaches: hidden dangers and causes

The current situation with healthcare data security is extremely dangerous, as patient health information can be sold or used for crimes such as identity theft and insurance fraud, or to illegally obtain prescription drugs.

Outsider threats continue to present new challenges, but hidden insider threats are even more dangerous.

Just take a look at the **2019 Data Breach Investigations Report** by Verizon. It says that privilege misuse and web applications are responsible for 81% of healthcare-related data incidents. Internal actors are responsible for 59% of all breaches in the healthcare industry.

Healthcare data breach statistics for 2018*



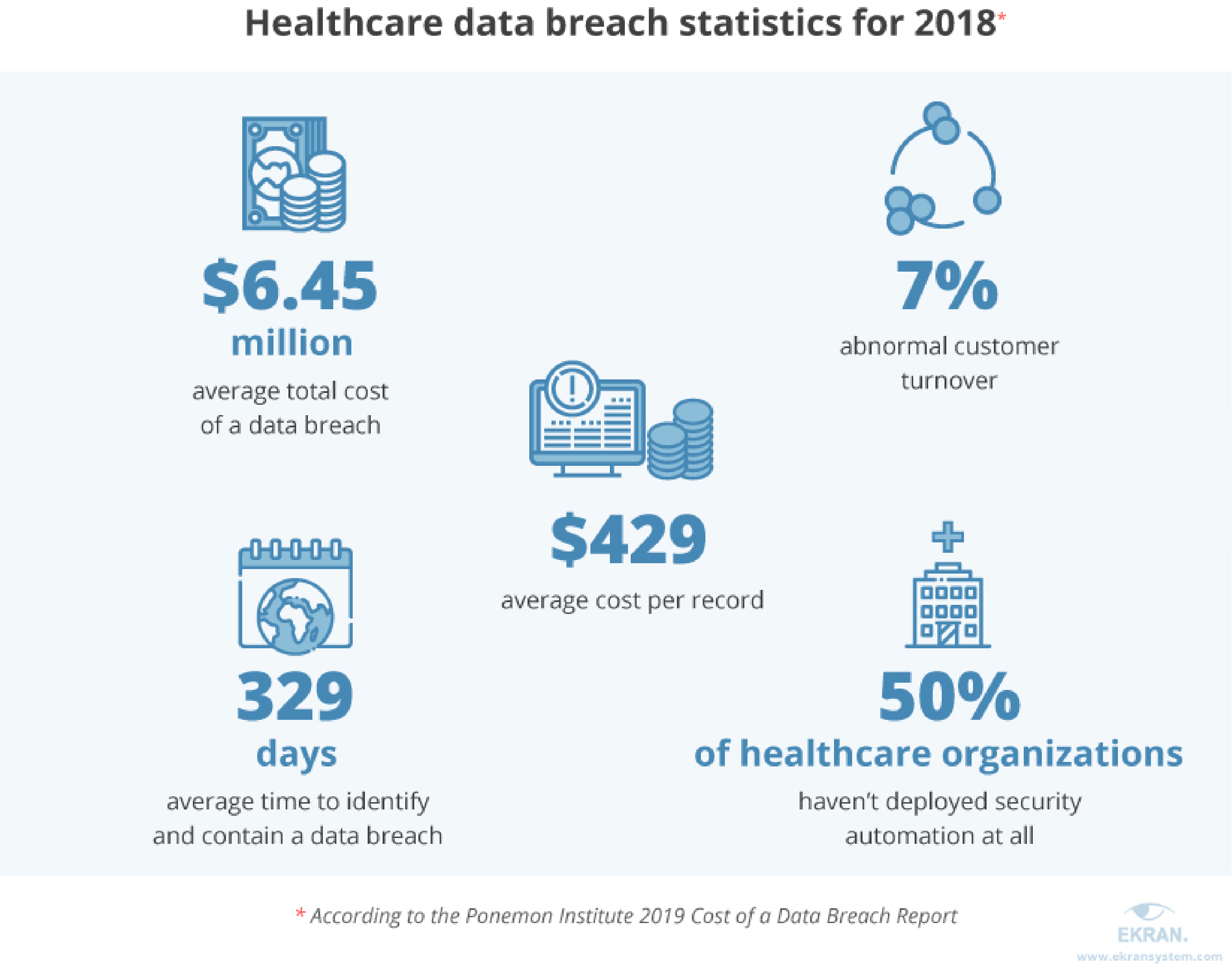
* *According to the Verizon 2019 Data Breach Investigations Report*

The cost of healthcare data breaches

Knowing the size of the problem, it's time to calculate its cost.

According to the **2019 Cost of a Data Breach Report** by the Ponemon Institute, for the ninth year in a row, healthcare organizations have had the highest average cost associated with a data breach at $6.45 million – over 60% more than the global average for all industries.

Not only does the healthcare industry suffer from the highest costs for data breaches – it also takes the most time to identify and contain them: on average, it takes healthcare organizations 236 days to identify a problem and 93 days to contain it.



Healthcare data breach statistics for 2018*

$6.45 million
average total cost of a data breach

7%
abnormal customer turnover

$429
average cost per record

329 days
average time to identify and contain a data breach

50% of healthcare organizations
haven't deployed security automation at all

* *According to the Ponemon Institute 2019 Cost of a Data Breach Report*

With all these numbers, it's no wonder that the Health Insurance Portability and Accountability Act (**HIPAA**) pay lots of attention to unauthorized disclosures of protected health information (PHI), improper disposal of PHI, unauthorized access to PHI by cybercriminals and rogue healthcare employees, and other IT security and privacy breaches.

HIPAA has also added a Technical Safeguards section to its **Compliance Checklist** so that organizations with access to electronic Protected Health Information (ePHI) can ensure software security.

Electronic Health Record systems: benefits and vulnerabilities

Knowing that hacking of healthcare organizations is on the rise leads us to the question of what exactly is lacking in healthcare software and how we can protect sensitive data.

Almost all healthcare providers use Electronic Health Record (EHR) systems to store and manage sensitive healthcare data, including the following patient records:

- Full name and birth date
- Bank account information
- Health data
- Social Security number
- Insurance information
- Contact information
- History of visits to healthcare professionals
- Hospitalization records
- Allergies and immunization status
- Family history
- List of prescribed medications
- Medical images

The EHR initiative was born thanks to the Health Information Technology for Economic and Clinical Health Act (**HITECH Act**).
Benefits of EHR systems are enormous:

- Streamline workflows
- Consolidate all data in one place
- Improve care coordination
- Reduce healthcare disparities
- Automatically update information
- Share information among offices and organizations
- Share media like medical images

However, EHR systems have several significant downsides when it comes to healthcare data security:

- **Consolidated data** poses a great security risk. If perpetrators get access to the system, they can get full control over a wide range of personal patient data.
- Apart from patient records, healthcare software can contain **financial information**, which attracts cybercriminals.
- **Phishing attacks** may cause severe damage to data security if healthcare professionals aren't taught how to identify them.
- **Malware and ransomware** can reach EHR systems via downloads, software vulnerabilities, and even encrypted traffic. This malicious software may cause harm not only by stealing data but also by locking users out of their computers and demanding payment to regain access.
- In healthcare, **insider threats** come from medical staff. Employees can cause trouble on purpose (stealing information to sell it) or by accident (disclosing it because of lack of cybersecurity education).

Why the current approach has problems

Most data protection solutions in healthcare are focused on establishing and maintaining a security perimeter, but most attacks and security breaches happen from within the system.

Perpetrators can be either employees or criminals trying to get access to the system from inside the building – for example, by using a public Wi-Fi connection or a USB device. To protect patient information stored in hospitals and other healthcare organizations from such insider threats, an employee activity tracking solution is required.

Almost all popular EHR systems like Cerner, Epic, Allscripts, and CureMD have some user tracking features, allowing you to see who accesses sensitive data. However, such features have their own limitations and vulnerabilities.

- Usually, EHR systems don't record the actions of **users with privileged accounts**, such as administrators. This allows those users to carry out malicious activity undetected.
- Administrators can go undetected when **changing the entitlement level of any user,** including themselves. Thus, they can circumvent internal system monitoring and access personal patient data.
- Even if access to sensitive data is recorded, it's **impossible to know how the data was used.** Therefore, it's complicated to detect malicious actions in time and prove violations.

To overcome all these drawbacks of EHR systems, it's essential to use **tracking software** that monitors all user activity in compliance with the HIPAA audit checklist.

For electronic health record systems, auditing software that provides constant EHR system monitoring can significantly speed up the audit process, lessening your headaches and costs.

How can Ekran System secure your EHR software?

Ekran System provides **compliance** with various standards, including HIPAA. It monitors all user activity on servers and desktops, in applications, on webpages, and on any visible area of the screen.

Ekran System secures your healthcare software

As per HIPAA compliance requirements, Ekran System provides access control and can help you analyze risk and establish a clearance procedure. It can also be used to help you develop and deploy information system activity reviews as required by HIPAA.

- **Indexed session video records.** Ekran System records video of everything users see and do on their screens (with configurable quality). A YouTube-like player provides a Live Session View, keyword search, and multilayer metadata such as the current application name and opened URLs.
- **Automatic alerts on suspicious events.** The user and entity behavior analytics (UEBA) module in Ekran System uses an alert system and an artificial intelligence module to detect suspicious activity and alert you immediately. This feature also supports USB management: Ekran System logs USB device connections, alerts on connected devices, and blocks them with rules, whitelists, and blacklists.
- **Identity management.** Ekran System identifies all users with a secondary level of authentication, allowing you to distinguish between users who work under shared accounts. Two-factor authentication is employed for all users, including privileged ones.
- **Access management.** Ekran System provides privileged account and session management (PASM) to help you monitor and review all activities carried out by a privileged user, configure who can access what endpoints within a protected perimeter, and set up expiration and update dates for credentials.
- **Investigation tool functionality.** Broad reporting tools summarize various aspects of data,

including all user logins for an endpoint, visited URLs, and most and least used applications. You can painlessly export recorded sessions, episodes, and other results of a cybercrime investigation in a forensic formats.

Ekran System monitors and records the sessions of all users, including privileged and third-party users, so that you can review any access to and actions performed on sensitive data. Moreover, Ekran provides an access policy and report tools to extract evidence if needed by investigators.

The features offered by Ekran System allow you to know precisely who has access to patient data and how they're using it. These features can be used to organize timely incident response, identity theft and prevent fraud, and provide evidence in case of a criminal investigation.

Conclusion

With HIPAA in full force and costs of potential data breaches skyrocketing, the importance of reliable security is greater than ever.

Monitoring software provides the first level of defense against insider threats and will help you to stay on top of your security and compliance needs.

Ekran Systems allows you to:

- Mitigate vital vulnerabilities of popular EHR systems
- Secure personal data of your patients
- Track third parties and software service providers
- Ensure proper HIPAA compliance
- Ensure effective software deployments on both a small and large number of endpoints

Request a free demo and see how Ekran System can strengthen the cybersecurity of your healthcare institution and protect PHI.

BAKOTECH is an international group of companies, a flagship in focused Value Added IT Distribution that represents solutions of leading IT vendors. Positioning itself as a True Value Added IT distributor BAKOTECH provides professional pre-sales, post-sales, marketing and technical support for partners and end-customers. Geographically the Group operates in 29 countries covering Central, Western and Eastern Europe, the Balkans, the Baltic States, the Caucasus, Central Asia with offices in Prague, Krakow, Riga, Minsk, Vienna, Kyiv, Baku and Nur-Sultan.

To get more information about **Ekran System** solutions, please contact us at **ekran@bakotech.at** or visit **www.bakotech.at**