Ekran

Blog / Data Protection / How to Calculate the Cost of a Data Breach

Data Protection

How to Calculate the Cost of a Data Breach

Yevhen Zhurer
Head of Business Development

February 21, 2024

Share:

The financial consequences of a data breach can impact your organization in unprecedented ways. Entailing costly remediation measures and reputational damage, data breaches often amount to substantial monetary losses. But what factors contribute to the overall cost of a data breach?

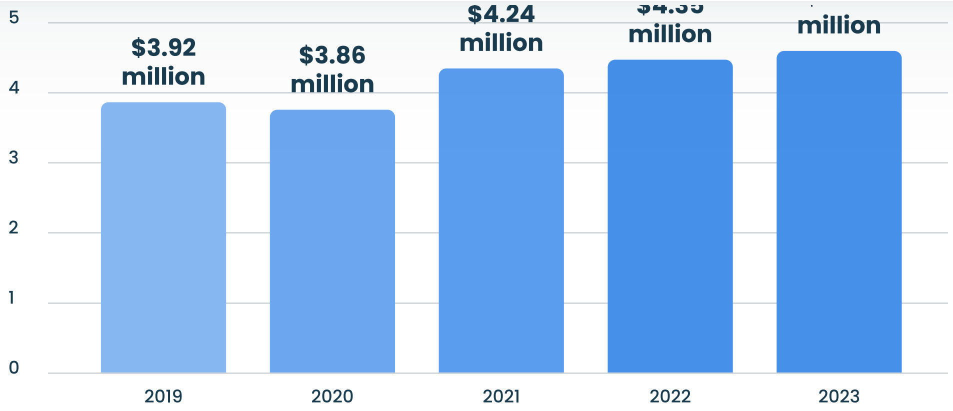
Calculating the financial cost of a data breach is a tricky process that includes estimating the total cost associated with all the consequences. In this article, we show you how to quantify the potential cost of a data breach and provide tips on preventing such incidents in your organization.

What is a data breach?

As defined by NIST, a data breach is “an incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.”

Data breaches usually affect the financial, medical, or personally identifiable information of individuals and organizations. A leak of such information can lead to financial losses — fines and penalties, remediation costs, loss of potential profits, investments in new security measures, loss of opportunities costs, and many other negative consequences.

The average total cost of a data breach keeps growing, reaching an all-time high of $4.45 million in 2023.



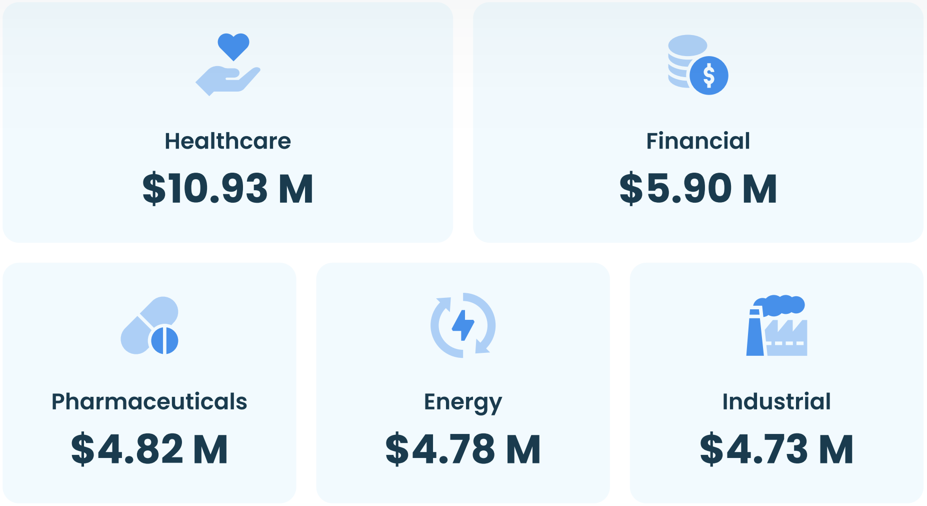
According to the 2023 Cost of a Data Breach Report by IBM Security

The frequency of data breaches is also on the rise. According to the 2023 Q3 Data Breach Analysis by Identity Theft Research Center, U.S. organizations reported 2,095 data breaches by October 2023, more than the total number of breaches that occurred over the entire span of 2022 – 1,774.

Now, let's delve into industries most affected by these data breaches.

Which industries suffer the most from data breaches?

Ponemon Institute in the 2023 Cost of a Data Breach Report analyzed data from 553 organizations affected by data breaches worldwide. The report reveals the top 5 vulnerable industries that experience the costliest data breaches – healthcare, financial, pharmaceutical, energy, and industrial organizations experience the costliest data breaches.



Healthcare	Financial
$10.93 M	$5.90 M

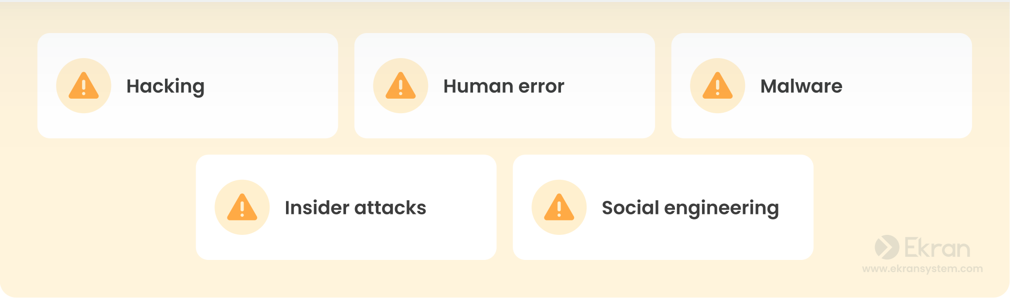
Pharmaceuticals	Energy	Industrial
$4.82 M	$4.78 M	$4.73 M

According to the 2023 Cost of a Data Breach Report by IBM Security

Notably, the average cost of a data breach in the healthcare industry has grown 53.3% over the last three years, increasing more than $3 million from $7.13 million in 2020. Below, we explore the main reasons behind these data breaches and the increase in their cost across industries.

What are the top causes of data breaches?

According to Verizon’s 2023 Data Breach Investigations Report, 74% of breaches involve a human element. Besides employee negligence, data breaches involve external attackers accessing an organization’s network through stolen credentials, phishing, and other techniques.



1. Hacking. Organized cybercrime continues to be one of the most widespread causes of data breaches. Hackers aim to steal sensitive data and either sell it or use it for their own benefit. The most common methods of hacking include DDoS attacks, credential theft, use of backdoors, command and control attacks, and brute forcing.

2. Malware. Malicious software like ransomware, spyware, Trojans, and downloaders enables cybercriminals to obtain sensitive data or the credentials of trusted user accounts. Malware can be delivered to a user’s computer via an email, messenger, compromised website, or compromised device.

3. Social engineering. This type of malicious activity is aimed at obtaining user credentials or other sensitive information without hacking. It often involves impersonating trusted parties to trick people into giving up sensitive information or taking harmful actions. Common forms of social engineering include phishing, email compromise, phone calls, and pretexting.

4. Human error. People within organizations may send emails to the wrong recipients, upload sensitive data to public cloud storage, or misuse their privileges. The average annual cost to remediate incidents caused by negligent insiders is $7.2 million according to the 2023 Cost of Insider Risks Global Report by Ponemon Institute.

5. Insider attacks. This type of attack is caused by a user with legitimate access to sensitive data: a disgruntled employee, a third-party vendor, or a malicious inside agent. Insiders are usually more dangerous than external threat actors since they know exactly what data they can obtain and they have access to the network.

Moreover, insiders’ actions can stay unnoticed and silently harm the organization for a long time because insiders usually know which security tools are deployed and how to overcome them. No wonder from hacktivism, revenge on the company, and government espionage.

What are the most damaging data breaches of 2023?

The cost of a data breach greatly depends on the number of compromised records, their type, and the time it takes to contain the breach. According to the 2023 Cost of a Data Breach Report by IBM security, the customers' and employees' personally identifiable information (PII) was the most commonly breached and the costliest type of record — approximately $183 and $181 per record respectively.

The same report also shows that a longer-than-average data breach lifecycle is associated with higher costs — $4.95 million (more than 200 days) vs $.3.93 million (less than 200 days of the data breach lifecycle). Yet, the most notorious cybersecurity incidents of 2023 cost even more than that.

- The mass hack of the popular file transfer tool, **MOVEit**, has impacted more than 1,000 organizations and more than 80 million individuals worldwide as of August 2023. British Airways, Based on the average cost of the data breaches and the number of records affected, the estimated total cost of this attack has reached about $9.9 billion so far. This places the MOVEit breach among the farthest-reaching attacks of 2023 and one of the largest data heists in recent years.

- Another infamous case is that of **T-Mobile**, one of the largest 5G networks and mobile carriers in the United States. T-Mobile suffered three data breaches in 2023; the first one took place in January of that year and affected 37 million customers whose PINs, phone numbers, full names, dates of birth, and addresses were revealed.

  The second one happened in April 2023 and impacted 836 customers whose data had been compromised — Social Security numbers, government ID data, and T-Mobile account PINs. That year's September breach involved the data of T-Mobile employees — 89 gigabytes of employee data, including email addresses and partial Social Security numbers, were posted on a hacker forum.

  These incidents are only part of a series of data breaches that T-Mobile has experienced in recent years. For example, breaches in 2022 cost the company $350 million — and that's just in customer payouts.

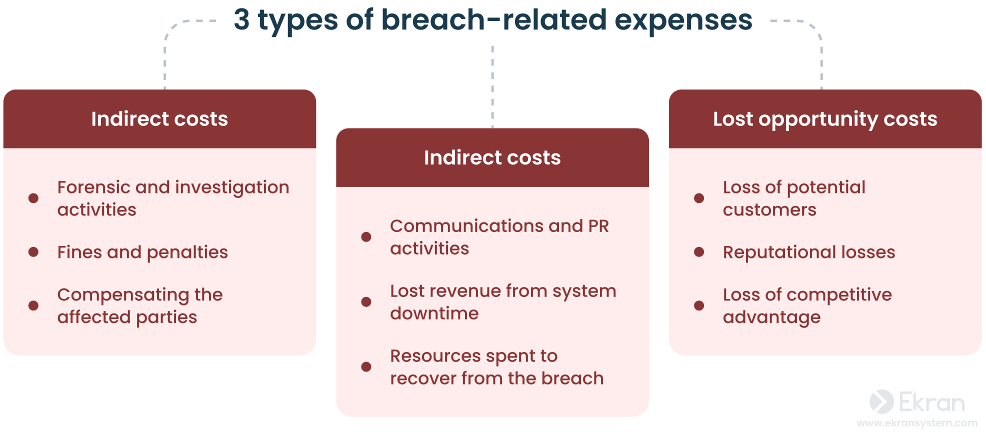
- Among the other big data breaches of 2023, we must mention the cyber attack on **Yum! Brands**, which took place that year on January 18. As the result of unauthorized access to Yum! Brands' networks including KFC, Taco Bell, and Pizza Hut, malicious actors stole and exposed employees' personal information including their names, ID card numbers, and driver license numbers. Cybercriminals also disrupted the IT systems, which led to the temporary shutdown of approximately 300 restaurants within the UK.

  Yum! Brands said that the corporation had "incurred, and may continue to incur, certain expenses related to this attack including expenses to respond to, remediate, and investigate this matter".

within your organization, let's dive deeper.

What determines the cost of a data breach?

Determining the costs of a data breach involves calculating several major components:


3 types of breach-related expenses
Indirect costs
Forensic and investigation activities
Fines and penalties
Compensating the affected parties
Indirect costs
Communications and PR activities
Lost revenue from system downtime
Resources spent to recover from the breach
Lost opportunity costs
Loss of potential customers
Reputational losses
Loss of competitive advantage
Ekran
www.ekransystem.com

- **Direct costs** of a data breach are the expenses for dealing with a detected breach. This includes the costs of forensic activities and information security investigation, fines, and compensating the affected parties.
- **Indirect costs** are connected with the time, effort, and other resources necessary to cover losses from the data breach. Indirect costs of data breaches include expenses for communications regarding the status and effects of the breach; issuing new accounts, credit cards, and credentials; and lost revenue from system downtime.
- **Lost opportunity costs** account for lost business opportunities as a consequence of reputational harm. For example, a breach can lead to a loss of potential customers, a shortfall in profits due to a loss of reputation, or the loss of a competitive advantage in the market.

million, whereas in Germany it was $4.67 million, and in Australia it was $2.70 million.

What factors form the cost of a data breach?

Each data breach does a varied amount of damage and needs to be handled differently. In the 2023 Cost of a Data Breach Report, IBM Security highlights the following key factors for estimating the cost of a data breach:

Factor	Description
Type of affected data	Compromising records of customers' PII, employees' PII, intellectual property, and other sensitive corporate data cost the most — $183, $181, $168, and $156 per record respectively.
Number of affected people	Each person affected by the breach needs to be compensated. The larger the scale of the breach, the higher the cost to fix it.
Attack vector	Some attack vectors provide malicious actors with more ways to harm an organization than others. On average, the most expensive attack vectors are malicious insider activity ($4.90 million), phishing ($4.65 million), and business email compromise ($4.67 million).
Duration of the breach	Breaches that are detected and remediated in less than 200 days on average cost organizations $3.93 million, whereas those that last over 200 days cost $4.95 million. That's a 23% difference.

	incident response programs.
Security automation and artificial intelligence (AI)	Leveraging AI and automation helps stop a security incident in its early stages, helping companies save on average $1.76 million per data breach.
Data anonymization	Anonymized customer data on average costs less compared to other types of data — $138 per record.
Complexity of the cybersecurity system	Organizations with more tools, systems, devices, and users experience an average cost of a security breach of $5.28 million, compared to $3.84 million for organizations with low system complexity.
Use of different environments	Companies that store data in the cloud — public, private, or multiple environments pay $4.75 million for a data breach, which is 6.74% higher than the average cost of a data breach.
DevSecOps adoption	Organizations with high DevSecOps adoption levels experience the largest cost savings. They save on average $1.68 million compared to those with low or no DevSecOps adoption.

As you can see, many factors can influence the cost of an organization's data breach, and calculating losses must be handled on a case-by-case basis. However, there are common methods that can help you quantify the cost of a data breach.

How to calculate the cost of a data breach?

effective ways to estimate the cost of a data breach for your own company more or less precisely.

Activity-based costing (ABC) method

The activity-based costing (ABC) method is widely used by Ponemon Institute for its reports. This method requires you to identify and estimate the cost of all the activities in your organization needed to resolve a data breach. This method categorizes more "indirect costs" as "direct costs" compared to conventional cost analysis.

Activities needed to resolve a data breach according to Ponemon Institute

Discovery and the immediate response to a data breach
Activities conducted in the aftermath of discovery
Conducting investigations and forensic analysis
Referring to audits and consulting services
Determining the victims of the data breach
Involving legal services for defense and compliance
Organizing the incident response team
Offering free or discounted services to victims

Providing identity protection services
Preparing notices and other documents for data breach victims and regulators
Calculating customer churn or turnover
Implementing call center procedures
Paying for customer acquisition and loyalty programs

Factor analysis of information risk (FAIR)

Another useful approach actively used by Ponemon Institute is factor analysis of information risk (FAIR).

> **“The FAIR risk quantification methodology can help ascertain the probability of security incidents and calculate the associated costs in business value.”**
>
> The Cost of a Data Breach Report 2021 by IBM Security [PDF].

The FAIR model is based on a taxonomy of the risk factors and how they affect each other. Its aim is to quantify and manage the risks in your organization. The main stages of FAIR analysis include:

FAIR framework

Evaluating threat event frequency

Estimating loss event severity

Determine the potential financial impact — the cost of recovering from the breach, fines and/or legal liabilities, and the possible loss of customers or revenue.

Assessing single loss expectancy

Consider the expected financial loss from a single data breach.

Calculating annual loss expectancy

Project the expected financial loss from data breaches over a year.

By using the FAIR framework, you can get a clear picture of the financial risks associated with data protection within your organization and take effective measures to mitigate those risks.

Data breach calculator

Probably the easiest method is using dedicated data breach calculators like:

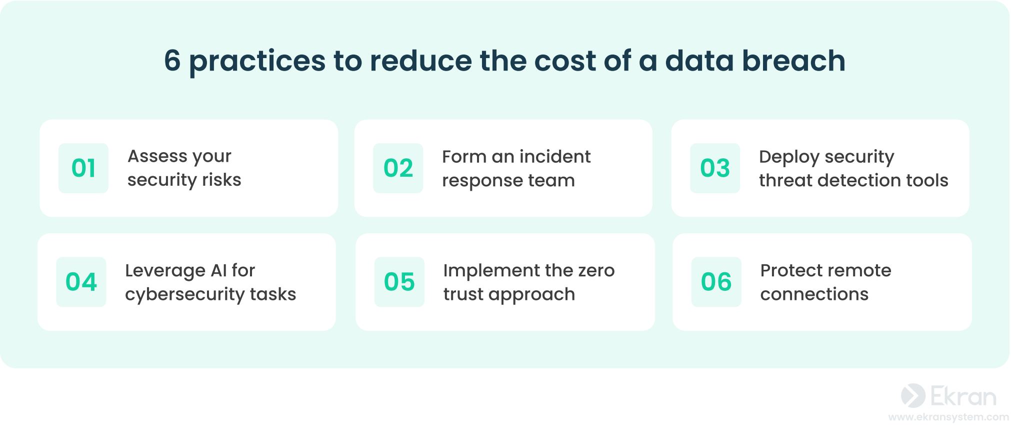
- NetDilligence sample calculator that relies on public information and data from various websites that track breach statistics
- HIPAA Secure Now! Calculator designed for healthcare organizations.

Take note that the outputs of these data breach calculators are estimates and actual data breach costs may differ. Though the cost of a security breach because each data breach needs to be handled in a different way. The type of data stolen, the size of the breach, its impact on your reputation, and some other aspects may become cost-forming factors.

If you agree that *prevention is better than a cure*, let's take a look at the best practices for reducing the risks associated with data breaches.

6 practices to reduce the risk of data breaches

The good news is that you can prepare for a data breach, mitigate possible damage, and reduce your expenses. Prevention of intellectual property theft and other data breaches involves reinforcing your cybersecurity system with the most efficient tools and practices.



6 practices to reduce the cost of a data breach

01 Assess your security risks

02 Form an incident response team

03 Deploy security threat detection tools

04 Leverage AI for cybersecurity tasks

05 Implement the zero trust approach

06 Protect remote connections

1. Assess your security risks

Before improving your cyber defenses, it's a good idea to find out what can harm your organization the most. To do that, you can conduct a risk assessment — a practice that helps you identify:

- Sensitive data

While conducting a risk assessment, it's useful to analyze known data breaches in your industry and the history of security incidents in your organization. To track the actions that may put your sensitive data at risk and prevent potential damage, use Ekran System — a full-cycle insider risk management platform. Ekran System's auditing and user activity reporting capabilities can provide useful insights into security incidents and their impact on your systems, helping you enhance your incident response activities.

Content

2. Form an incident response team

Forming a threat response team and implementing a robust incident response program can help you identify a data breach 54 days faster, thus significantly reducing its cost according to the 2023 Cost of a Data Breach Report by IBM Security. However, preparing an efficient team requires considerable effort.

An incident response team should include employees who can quickly remediate damage from the data breach if it occurs. They need to analyze the incident, gather evidence, take the necessary recovery measures, notify affected parties, etc.

To be able to respond to incidents swiftly and efficiently, the team should consist of specialists from various departments: IT, legal, security, communications, customer service, and executive management. The threat response team also requires relevant cybersecurity training, the authority to act decisively, and the opportunity to prepare incident response plans for various breach scenarios in advance. For more advice on establishing an effective incident response process, consider referring to NIST incident response planning tips.

3. Deploy security threat detection tools

Threat detection time plays a crucial role in determining the cost of a data breach. The more time a malicious actor handles your organization's data, the more damage they can cause. The most efficient way to detect security threats at early stages is by deploying dedicated software that monitors activity in your network and notifies you of any unusual and suspicious activity.

rules, Ekran System sends an alert to your security team. The security officers can then view the user's session online, determine whether the user's actions threaten your organization's security, block the user, and end the process if necessary.

To make incident response even more efficient, you can configure Ekran System to block suspicious activities automatically.

4. Leverage AI for cybersecurity tasks

Implementing AI capabilities takes security threat detection to another level. AI allows security officers to take preventive actions against potential threats, reducing the mean time to identify and contain a breach by 108 days and, thus, saving approximately $1.76 million on a data breach according to the 2023 Cost of a Data Breach Report by IBM security.

AI is the core of user and entity behavior analytics (UEBA) solutions that analyze daily user activities, create a baseline of user behavior, and spot any changes and unusual actions. UEBA solutions can also help security officers assess threats by analyzing each user's actions and calculating a risk score. A UEBA tool can detect sophisticated data breaches caused by:

- User account compromise
- Credential leaks
- Malicious insider activity.

5. Implement the zero trust approach

As the name suggests, the zero trust approach to cybersecurity assumes that no user or entity in your system should be trusted by default. Users should be able to access only the resources they need for their work routines. Additionally, before providing a user with access to resources, you should verify their identity.

This approach helps to significantly reduce the attack surface in case a user acts maliciously or their account is compromised. That's why organizations with a mature zero trust architecture in place can lower the average cost of a data breach by $1.51 million, according to the 2022 Cost of a Data Breach Report by IBM Security [PDF].

You can implement the zero trust approach by leveraging Ekran System's identity and access management capabilities. With multi-factor authentication, it's easy to verify user identities and reduce the risk of unauthorized access.

Moreover, Ekran System helps you secure access to sensitive data with the following functionalities:

- Privileged access management
- Time-based access restrictions
- Manual access approval
- Auto-generated one-time passwords, and other methods.

6. Protect remote connections

The switch to remote work has reduced the effectiveness of organizations' IT defenses. In 2022, this resulted in an almost $1 million increase in the average cost of a breach, according to the Cost of a Data Breach 2022 Report by Ponemon Institute [PDF]. As more and more remote employees work outside of traditional on-premise environments, use unprotected devices, and connect to unsecured public networks, they pose additional security risks to organizations.

However, you can mitigate these risks by:

- Securing connections to sensitive resources with a VPN

workers in your IT infrastructure
- Limiting access to sensitive resources with Ekran System's PAM functionality
- Verifying every user's identity upon each connection.

Conclusion

The cost of a data breach depends on a great number of factors. Every breach is unique, making it difficult to pinpoint how much a data breach could cost your company. In this article, we have described the best techniques for calculating the possible impact of a data breach on your organization. Nevertheless, it's always best to take a proactive approach to prevent data breaches. In this article, we have provided the best security practices to help you reduce the risk of a data breach and avoid its negative consequences.

By building a mature incident response program, following zero trust principles, and securing your endpoints with dedicated software, you can significantly fortify your defenses and prevent leaks of sensitive data. Ekran System helps you detect and put a stop to security breaches with robust user activity monitoring, access management, and incident response functionalities.

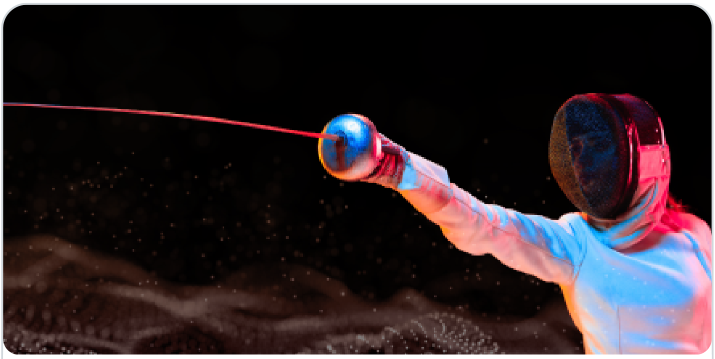
Want to try Ekran System? Request access

Ekran

Access the Demo Portal

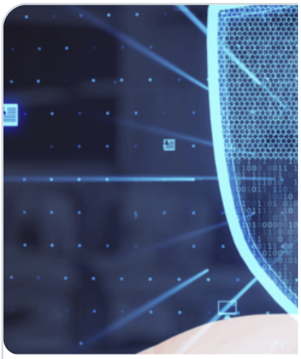
Share:

Trending articles



Security 13 September 2023

How to Build an Insider Threat Program [10-step Checklist]



Security

12 Cybersecu Measures to F Attacks in 202

Stay up-to-date with the cybersecurity news, insights, and best practices delivered straight to your inbox

Business Email*

First Name*

Last Name*

□ I have read and agree to the Privacy Policy. I agree to receive periodic emails containing product updates, exclusive offers, as well as newsletters about Ekran System products and services and industry insights. *

Subscribe

See how Ekran System can enhance your data protection from insider risks.

Access the Demo Portal

Request a Free Trial

60 Kendrick St. Suite 201
Needham, MA 02494, USA

+1 781-205-0530

Contact Us

D-U-N-S number: 089270023
CAGE number: 88VL6

Terms of Use EULA Terms of Service

CYBER ESSENTIALS
CERTIFIED

Ekran