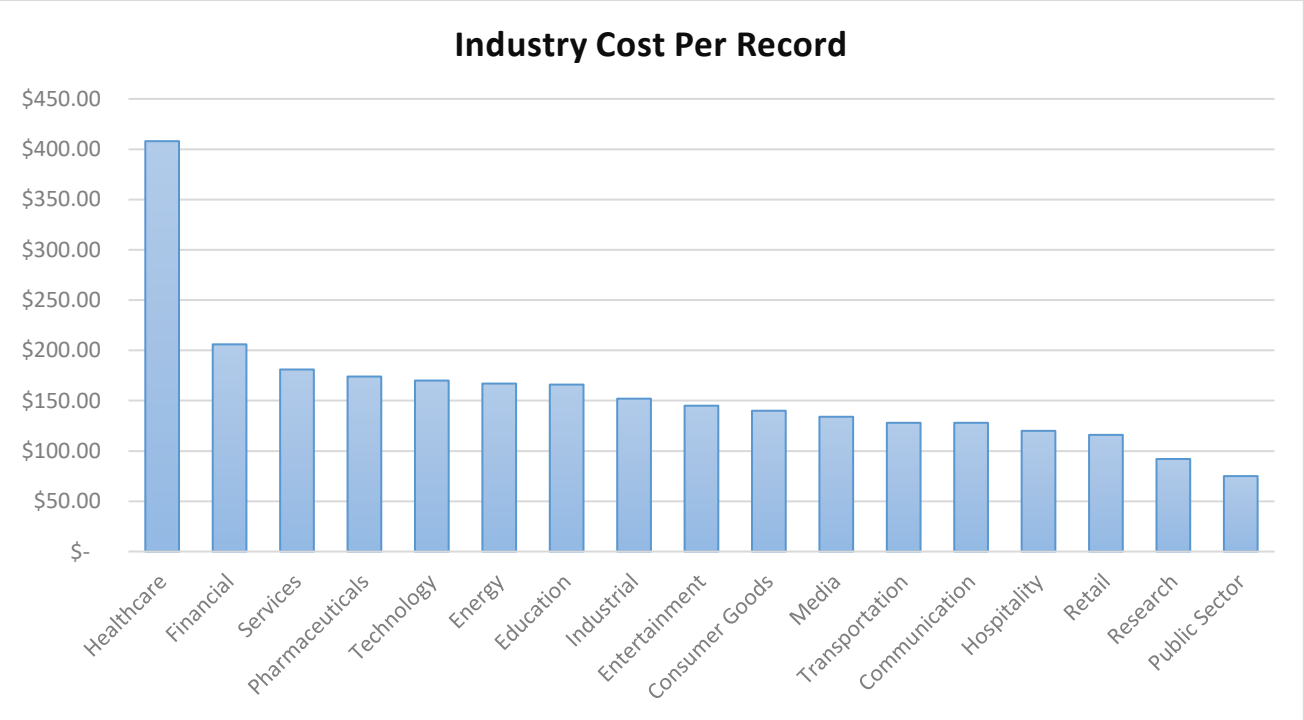
Cost of Data Breach

Personal data is the pillar of our society and the "secret sauce" of important elements of our day-to-day ingredients. Costs and risks of data breaches are increasing (and they are)! We need a radical shift in our tactics to data protection and network security.

According to the latest Ponemon annual report, the average cost of a data breach is currently $3.62 million globally, which comes to $141 per record.

In the U.S., the cost is almost double that, at $7.35 million. "We can't decide what to do, we can wait, this will not happen to a small organization like us…" This type of thinking must change. We are at a tipping point on the implications of data breaches. The costs have become more real to companies and the boards who run them. CEOs and executives are now losing their jobs because of data breaches.



Data protection begins with real and measurable commitments. This commitment includes non-technical and technical data protection. This is a fine balancing act. You have to have the proper protections and people buy-in, with reasonable and appropriate processes. These factors should not impede on your network speed or efficiency.

Non-technical

Proper Due Diligence – Trust but verify. Companies need to carry out proper due diligence. This includes assessing, testing and validating the internal skillsets of your IT team. If your team is worried about politics rather than security and efficiency, we have major problems. Team/Company: You should assess and determine if your security employees have the skills to work on an upcoming project, or if you need to bring in security experts.

Culture – Part of data protection contains embracing and harvesting a culture of security and privacy awareness. Your employees should be required to agree to and sign off on security policies, including a user data privacy policy, computer/device use policy, and BYOD policy before access is granted.

Training – Mandatory security and privacy training for new hires as well as annual follow-up training should be implemented. Regular awareness training should be regular events. That way, you can educate your employees on new attack vectors, phishing, and malicious social engineering attacks.

Technical

Minimization of Data Processing – Reducing the footprint of your protected data (collection, use and disclosure) is one of the best practices. Data processing should only use as much data as is required to successfully accomplish a given task. Additionally, data collected for one purpose should not be repurposed without further consent.

Edge-to-Edge and Layered Security – These strategies are as old as time, but these two combined principles will better your data protection. Edge security stands in contrast to enterprise security platforms, whose centralized nature make them easier to attack and compromise.

Edge to Edge: By decentralizing security to the edges–the devices people use–protecting data becomes more effective. Current platforms rely on securing servers that contain sensitive data, but these servers are central points of failure and have been hacked multiple times over the years, resulting in billions of dollars' worth of data being stolen.

Layered Security: This is also known as defense-in-depth. This is the practice of combining multiple controls to protect resources and data. This technique protects computer networks with a series of defensive mechanisms.

Assessment - Sound data protection starts with a full risk assessment of the infrastructure, including holistic technical testing, penetration tests, web security, social engineering tests, configuration reviews, standards, and people and process reviews.

You need to have a solid understanding of your cyber baseline before you begin to address any issues with it.

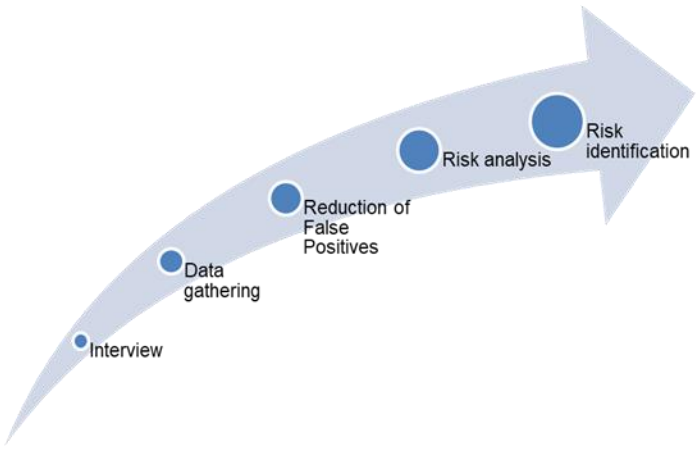
Persevere with tactical and strategic security goals and objectives: As your company continues to carry out its data protection, it will need a multi-year development plan that focuses on the network and a cybersecurity strategy that will evolve as security challenges are constantly evolving.

A detailed risk assessment should include the following scope:

- Data breach risk analysis
- Assess your organization's Administrative Security Safeguards
- Assess your Physical Security Safeguards
- In-depth evaluation of your Technical Security Safeguards

The assessment should include an internal and external network vulnerability assessment, including email security, LAN, application security, WAN, and web application security. Sanctioned social engineering acts should be included in the scope of the assessment.

A thorough process for documenting the review should be included in this process to assess the policies, procedures, templates and other relevant documentation related to your data security controls.



For an effective security risk assessment, the stakeholders' buy-in is important. Data accuracy from the network and applications will make or break the assessment.

Less false positives will lead to an accurate risk analysis and precise data for risk identification.

Companies should hold risk mitigation meetings at least once a quarter to present your stakeholders with "the good, the bad, and the ugly."

- **The good:** Security issues that were successfully dealt with during the previous quarter
- **The bad:** Any ongoing issues that have arisen and are being resolved
- **The ugly:** What has happened to others in the industry whose security strategies have been compromised and what can be learned from their failures