Handling Data Breaches

Devin Kennedy

Moraine Park Technical College

IT Administration

[REDACTED]

October 05, 2025

Data breaches have been an ever-rising threat since the first major breach back in 1984. A data breach is defined as any security incident where an unauthorized party gains access to sensitive or confidential information. This information can include, but is not limited to, Social Security Numbers, trade secrets, or even military plans. The impact can be costly, financially, legally, and reputationally. A single data breach can cost millions, with the average costing over four million dollars. There are laws and frameworks to be followed to help mitigate the risk. But bad actors are always lurking for a way in, be it through stolen credentials or with new threats like AI-assisted attacks. This paper will break down the background and landscape of these threats, the importance of a full, well-trained staff, the best practices for both preventing and responding to a data breach as well as how the size of the organization can affect them.

Background

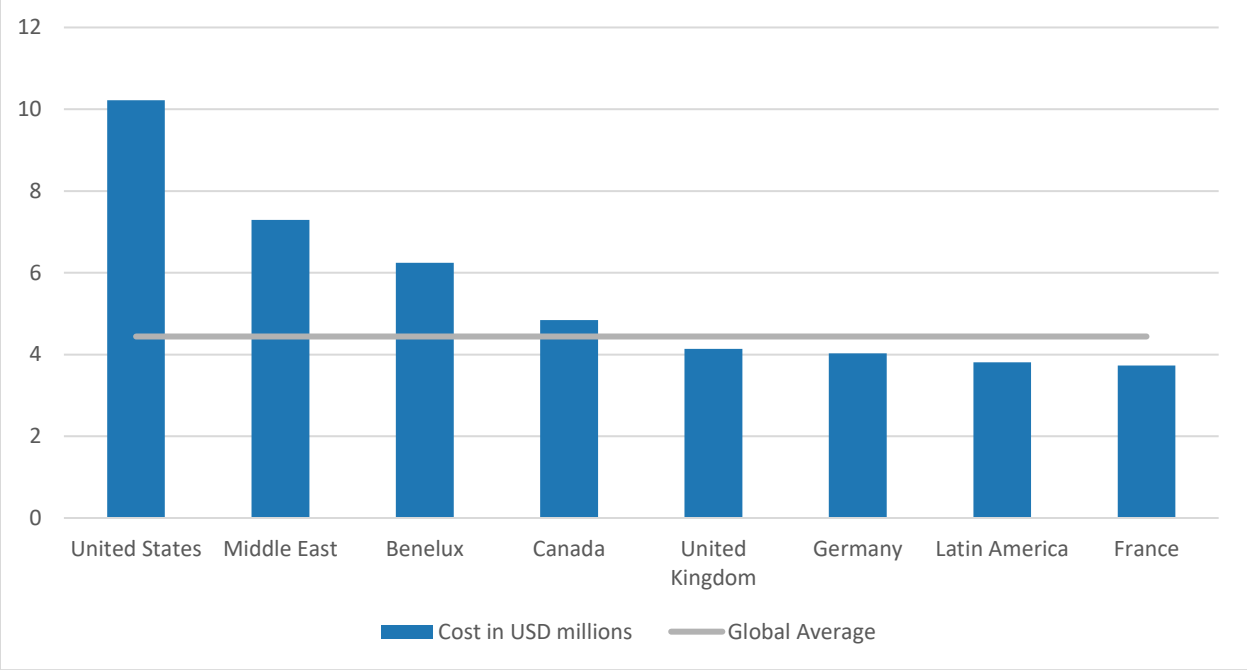
Not all cyberattacks are breaches. For example, a Distributed Denial of Service (DDoS) attack may have intent to simply disrupt an organization and not be a breach. So then, what is a data breach? A data breach is defined as being any security incident where an unauthorized party gains access to sensitive or confidential information. This information can include personal data such as your Social Security Number (SSN), banking information, or health information. It also includes corporate data such as intellectual property, trade secrets, financial information, and customer records potentially including credit card numbers. This data can be compromised through several methods with phishing and stolen credentials remaining the number one way bad actors gain access. But not all breaches involve hackers gaining access. Sometimes a breach can happen due to something as small as a thumb drive or piece of paper being stolen and falling into the wrong hands.

A stolen piece of paper was the basis of the first notable data breach. In June of 1984 TRW Information Systems reported that the credit history of some 90 million Americans had been exposed. Employees at a Sears Roebuck & Co. store in Sacramento, CA had been using a pad of paper to store the

passcode to access the credit reporting agency. This information was posted on an electronic bulletin board for a month before TRW was tipped off to it. Fast forward four decades later to January of 2024 and the largest data breach by size of data has occurred. Named the “Mother of All Breaches”, or MOAB for short was discovered by Bob Diachenko, security researcher at Security Discovery. His findings showed that 12 terabytes of personal data from 3,876 sites were being stored by a data breach search engine called Leak-Lookup and became accessible because of a misconfiguration with a firewall.

Data breaches don’t have to be that massive or noteworthy to carry massive consequences. According to IBM’s Cost of a Data Breach, the global average cost of a data breach is USD 4.44 Million, with the average cost in the US is 10.22 million dollars.

Figure 1



Average cost of a data breach in selected countries compared against the global average, per IBM’s 2025 Cost of a Data Breach Report

The cost can be affected drastically by what country the breach happened in as well as the field of the company that got breached. Financial organizations and healthcare have heavy regulations and fines

attached to them that raise the cost substantially. Fines aren't the only cost involved with breaches, of course. There are costs involved from lost business, both from downtime as well as lost customers, which amounts to $1.38m on average. The cost of detecting and escalating the incident averages to $1.47m. Expenses after the breach is contained average $1.2m. These costs include fines, settlements, legal fees, and providing free credit monitoring to affected customers.

There are several laws in the US and globally that contribute to those fees. Those laws also outline how and when breaches need to be notified to authorities and affected parties. The Health Insurance Portability and Accountability Act (HIPAA) outlines that the organization must notify the Department of Health and Human Services (HHS), affected persons, and potentially the media. US Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) says that finance, national security, and other designated industries must report a breach to the Department of Homeland Security (DHS) within 72 hours. EU's General Data Protection Regulation (GDPR) has a similar 72 hour requirement for any company in ownership of data belonging to EU citizens, even if the company is not based in the EU. All 50 U.S. states also have their own regulations regarding notifying the appropriate parties within specified timelines. With this foundation of what constitutes a data breach and its consequences, the next step is to examine who is committing breaches, how they're carried out, and why.

Threat Landscape & Vulnerabilities

The first step to understanding, and preventing, data breaches is to understand who it is doing it. According to Verizon's Data Breach Investigations Report (DBIR), on a global scale, 81% of breaches come from outside threats with internal employees making up 18%, and trusted partners and third parties making up 1.2%. But here in North America, those numbers shift dramatically with 91% being external, 5% for both internal and partners. One percent had multiple sources, which is why those numbers add up to 101%. According to 2019's DBIR, state-sponsored actors were behind 23% of breaches and 39% were tied to organized crime syndicates.

All those different attackers do it for different reasons. But there is one reason that's much more common, and expected, than the rest. Money. Financial motives were found in a massive 89% of breaches. That money comes from three main methods: ransomware being paid out, selling the stolen data on the dark web, and from using it to commit identity fraud. The next most common motive is for espionage, both corporate and state, making up 17% of motives. This 17% is more than double that of last year's report with a 163% increase. Unsurprisingly, motivations look quite a bit different when looking at just state-sponsored attacks. Almost three-fourths (74%) have espionage as the primary motive. Financial gain takes more of a backseat here, as the money is typically used to keep their operation running. Dishonest companies may steal trade secrets for a competitive edge. Nation-state actors will target government bodies to gain information on sensitive political dealings, military operations or national infrastructure.

After identifying threat actors and their motives, attention shifts to how they gain access. Intrusions are usually intentional; threat actors conduct reconnaissance to identify exploitable vulnerabilities, whether system misconfigurations or human factors, and then operationalize those findings to carry out an intrusion. Exploitation of vulnerabilities grew by 34% over last year to now make up 20% of breaches, while credential abuse edges it out for the number one spot at 22%. Phishing takes third at 16%. In that same report, it states that 65% of Internal actor breaches were caused by miscellaneous errors, while privilege misuse made up 31%. The biggest growing threat towards data breaches is the rise of Artificial Intelligence. Malicious emails that were assisted by AI doubled from 5% in 2023 to 10% in 2025. According to IBM, the time needed to craft a convincing phishing email has been reduced from 16 hours down to 5 minutes, or 192 times faster. 16% of breaches involved AI, with 37% being AI-Assisted phishing and 35% being deepfake impersonation. The impact of these evolving threats is not uniform: small businesses and large enterprises face very different risks, attack patterns, and constraints in responding to breaches.

Impact and Constraints Across Business Sizes

Every company is a target for data breaches, yet the methods of attack, the course of events, and the resulting impact vary significantly between small and large organizations. For the purposes of this paper, a small business is defined as a company with 1,000 or fewer employees and will be referred to as an SMB. SMBs are more prone to phishing, credential abuse and misconfigurations. SMBs also made up a staggering 82% of all ransomware attacks last year. SMBs made up 46% of all data breaches according to Verizon's 2023 DBIR. SMBs face a 350% higher rate of social engineering attempts. Large businesses, on the other hand, are more likely to be victims of system intrusions and compromised supply chains. Larger organizations are also more likely to be attacked with espionage as the motive.

SMBs are typically more heavily burdened by a breach than a large business would be. The average cost of a breach at an SMB ranged from $826 to $653,587 in 2020, totaling $2.8 billion. The average ransom was $700,000. Approximately half of SMBs are able to resume operations withing 24 hours. 51% of SMBs decide to pay the ransom, rather than fight it. SMBs have stricter budgets, and therefore cybersecurity funding is not always a high priority. About half of SMBs spend under $1,500 per month on cybersecurity, comprising between 5 to 20% of their overall IT budget. 17% have cyber insurance, the same percentage of SMBs that report encrypting their data. Some major security tools are being adapted more and more by SMBs, with antivirus software being the most common at 58%, firewalls and VPNs are a little behind at 49 and 44% respectively. Password managers are now being utilized by 39% of SMBs. Unfortunately, over half of SMBs have no formal cybersecurity measures in place and a little over a third report "no concern" on the matter.

Large businesses are more likely to bounce back from breaches even though their breaches can be exponentially more costly, due to having more robust security infrastructure in place. The median cybersecurity budget for enterprises is $5.7 million within an average of $41.8 million, or 14% of the overall IT budget. The cost of a breach is on average $4.44 million, with the healthcare industry

averaging $6 million. Their challenges come from a complex, broad attack surface, insider threats, and higher partner risk. Large businesses are starting to more widely adopt “Zero Trust” policies as well as AI detection and defenses. Having the correct resources at your disposal will only go so far. To get the most out of your defenses, you need a well-trained, well-staffed cybersecurity team.

IT Staffing and Professional Development

Even a fully staffed cybersecurity team will be of little use if it is lacking critical capabilities within its skillset. In 2024, more than half of organizations that experienced a data breach had stated that they were severely short staffed. This is a substantial 26.2 percent increase over the previous year. There is a direct link between short-staffed security teams and higher costs. The average cost of a data breach at an organization with a well-staffed security team was a little over half a million dollars less than that of a short-staffed organization. In many small businesses, there is no designated “cybersecurity” team, rather it’s just another hat the IT department must wear. In some small companies, there is no team, rather it’s just one IT person overseeing all their needs. Sam Hector, Senior Strategy Leader at IBM Security explained:

> Teams that are stretched too thin don’t have the time to devote to improving cybersecurity processes, integration and efficiency. They’re unable to drill exercises and embark on further training as they’re too focused on keeping the lights on. This means over time, they’re less effective compared to the threat landscape, and misconfigurations and gaps develop that attackers can exploit. (IBM, 2024)

Workers who continue to invest in their skills and keep certifications up to date are better able to weather economic uncertainty, while organizations who help them do so are less likely to experience skills gaps. Participation in regular security training can lead to a four times increase of reporting phishing emails. Training, such as taking classes, getting certifications, or attending workshops and seminars, is a great way to stay current in your skillset. It can also be beneficial in developing leadership skills, networking, and when looking for a career shift.

Continuous improvement is paramount for continuous success, both personal and for your company. Technology, and by extension, cybersecurity is a rapidly changing field. New technologies emerge daily, and along with them come a new set of threats and vulnerabilities. As things change, some remain the same. Stolen credentials remain the main way attackers get into systems. Human error is involved in approximately 60% of data breaches. These are often preventable mistakes if the company

establishes a culture of training and continuous improvement for all employees, not just the IT team. Some ways the IT department can foster that environment comes from the top down. Providing the team with the resources they need and clear expectations can lay the foundation. Being sure to provide feedback, support, and sharing knowledge, as well as encouraging that they get certifications can all go a long way. In my conversation with [REDACTED], IS Specialist at [REDACTED], he emphasized the need for continuous learning, saying that much of what he learned is “now useless”.

Best Practices for Prevention

One of the biggest trends in best practices for preventing data breaches is to adopt a zero-trust policy. The core concept of zero-trust is to never just assume that someone or something can be trusted. It should be verified every time, and if it cannot be verified it should be assumed to be an intrusion. One of the foundations of zero-trust is the principle of least privilege. This is the concept of establishing just enough access to resources to perform their job. This can be implemented through role-based and attribute-based access controls. Identifying and protecting high value assets ensures that those controls are applied to what is most important. Having a robust password policy is also important. CISA recommends that passwords have a minimum of 16 characters consisting of upper case, lower case, numbers, and special characters in a random order and are not to be used between multiple accounts. Secure passwords are not memorable though, which is why organizations are adopting use of password management tools that can store all of an employee's complex passwords into one secure location. CISA also says that multi-factor authentication (MFA) should be utilized in addition to complex passwords. There are three core types of authentication: Something you Have (a physical item such as a YubiKey), Something you Know (a PIN or One Time Passcode), and Something you Are (biometrics such as an iris or fingerprint scanner). Password managers and MFA can be very cost prohibitive for small companies, so an easier to remember solution is to use “passphrases” instead of more traditional passwords. These are a series of 4-7 unrelated words that can be, but do not have to be spaced out. Instead of relying on numbers and special characters to add complexity, their strength comes from overall length.

System hardening is a widely recognized best practice for protecting against data breaches. The National Institute of Standards and Technology (NIST) recommends reducing the potential attack surface by patching vulnerabilities and turning off nonessential services. Vulnerabilities aren't always apparent but still pose a risk. Unused services make the attack surface broader and more complex than necessary. The best way to harden a system is by using a dedicated host if possible. Install, deploy, and patch the operating system in a secure manner. A minimal installation with the necessary components added onto it later is ideal. Use an established process to prevent making mistakes that can compromise security. Systems should be audited regularly for unused components. Removing these unnecessary components has benefits beyond increased security. That can increase compatibility, free up system resources, and facilitate system monitoring. NIST hardening guide recommends the removal of the following services:

- Directory services
- Email services
- File sharing services
- Language compilers and libraries
- Network management tools
- Printer sharing services
- Remote access programs
- Remote control programs
- System development tools
- System management tools
- Web servers and services
- Wireless networking service

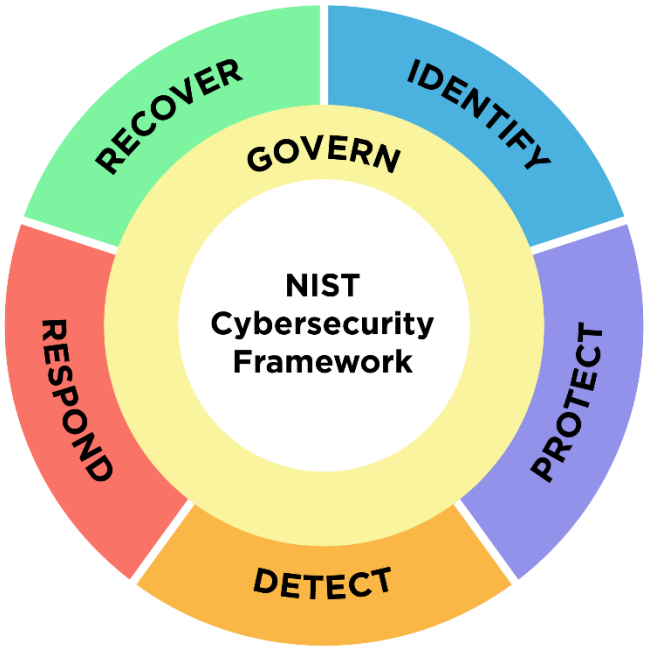
Configure user authorities as well. Removing all nonessential and non-interactive accounts should be done regularly. If the account cannot be removed entirely, but is not being used, it should be disabled.

As beguine as it may seem, make sure all devices are synchronized to a central, secure time source. This is important as time-drift as small as a few minutes can break Kerberos and give attackers a way in. Antivirus/antimalware software and firewalls (either physical or software) being purchased and installed is a great start, but they must be configured correctly to ensure optimal performance. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are fantastic ways to increase ways to harden a system. An IDS passively detects and alerts you to anomalies, whereas an IPS can actively prevent suspicious traffic from reaching its target like how a firewall operates. But because these systems add yet another cost to an already thin budget, usually $1,000 annually, and may seem redundant to systems already in place, many companies may not approve funding for them. Regular testing is essential, and if budget allows it hiring a penetration tester is a great idea.

Regular testing and training for all employees is important to make sure they stay current with knowing what threats they need to be aware of and may accidentally fall for. Running simulations such as fake phishing emails can help identify what threats are the biggest risk and who your most susceptible employees are so that you can tailor your training. Monitoring and detecting their activity can also be utilized to identify internal threats, be it malicious or accidental. Your third party partners and vendors also pose their own risk. A Third Party Risk Management (TPRM) system should be implemented to minimize the risk. This system should lay out a few best practices starting with laying out the organization's goals. Stakeholder buy-in is important to make sure that all parties are cooperating and sharing responsibility. A TPRM should help assess risk exposure, establish responsibilities to minimize these risks, and establish monitoring. A risk tiering model should also be used to classify the risk level and priority of third parties. A typical model is Tier 1—high risk, high importance, Tier 2—medium risk, importance, and Tier 3—low risk importance. Work with procurement as a part of your TRPM. Direct and indirect must be assessed as well as performing due diligence, vendor selection, contract negotiations, and ongoing monitoring.

There are several frameworks and guidelines that should be adopted depending on what the industry is, where the organization is, and who their customers are. One of the main frameworks is the NIST Cybersecurity Framework (CSF). It is still a recommended framework for any company, and as of 2017 was implemented as the standard for government agencies.

Figure 2



The NIST Cybersecurity Framework (CSF) wheel showing the five core functions.

This is a practical and flexible framework built on the functions of Identify, Protect, Detect, Respond, and Recover. There are four tiers of implementation: Partial, Risk-Informed, Repeatable, and Adaptive. The other major security framework that may be implemented is ISO/IEC 27001. It is an international organizational standard whose core concept is to protect the CIA triad. This refers to making sure that the organization's data maintains confidentiality, integrity, and availability. It is broken into two main parts: Clauses and Annex A. The 11 clauses are the actual requirements for what needs to be met to be compliant. Annex A consists of 93 controls which are the specific steps to be taken to satisfy those requirements. Alongside a solid framework, there are plenty of guidelines that must be followed

depending on what the industry is and where the clients are located. HIPAA is the 1996 US federal law that sets outlines for how protected health information (PHI) is protected. This law applies to any organization or person that handles PHI, including healthcare providers, insurance companies, and any other third party that may handle PHI such as a data center or billing service. It outlines how the data must be stored, access controls, and training that must be met to be compliant. The General Data Protection Regulation (GDPR) is a 2016 law enacted by the European Union setting strict data protection for all EU citizens. This law applies to any company that is in ownership of data of an EU citizen, regardless of where the company is located. It outlines that informed consent about what information is collected and stored should be implemented as well as only storing data that is necessary. GDPR is known for enforcing adequate handling and accountability through high fines.

Best Practices for Response

An effective response to a breach begins with clear communication and a laid out plan of action. That plan should begin with an Incident Response Plan, or IRP, that lays out what steps should be taken before, during, and after an incident has occurred. The IRP should be enacted and tested before a breach occurs. Detecting a breach as early as possible is critical. Use monitoring and logging system to recognize an incident early. This can come in the form of Security Information and Event Management tools, an IDS/IPS, and endpoint detection. The next step is to react to the breach immediately. The IRP should establish a designated team of roles of who to notify, and what they'll be responsible for. The Incident Manger will oversee the response and coordinate the teams. A communication manager will handle communicating with employees, clients, and PR/media. The technical lead will oversee investigating the breach and immediate fixes. A legal team should be notified to advise on any applicable laws that need to be followed. Figure 3 illustrates a typical escalation flow, showing how an incident moves from initial detection through the response team and leadership to regulatory notification.

Figure 3

Escalation flow for incident response communication from detection to regulatory bodies

As soon as everyone is notified, the affected system needs to be isolated to contain the spread. With initial reactions settled, the situation can now be evaluated. This is where you should be gathering and documenting every available log, a timeline of events, the detection method, communication, and containment and recovery processes. Once the root cause has been identified and contained, you will need to delete malware and any artifacts it leaves along with any scripts or backdoors. You need to patch out any vulnerabilities that were exploited and reset any compromised credentials. Test the systems to ensure it got eradicated properly. When the breach has been eradicated and systems are ready to be recovered, some best practices should be to restore back to a known safe backup and monitor it closely. Documentation of every step taken is critical. Once everything is back online, it is a good idea to have a formal meeting, often referred to as a "postmortem", with all appropriate parties to go over what lessons were learned. This is the best time to sit down and revise any policies and procedures that need to be updated to reduce the risk of this happening again.

Once everything calms down, one of the parties you'll need to contact is your cybersecurity insurer and file a claim if you already have an insurance plan. If you don't, now may be a good time to reconsider. Cybersecurity insurance can be a relatively affordable plan with the average cost for small businesses being $145 per month, with about one third of plans being under $100 per month. For enterprises, that price can be as high as $5,000 per month, though I could not find definitive confirmation. This insurance plan usually helps cover the costs associated with a breach or other cyberattack. These policies may cover costs associated with:

- Notifying customers

- Recovering personal information
- Data recovery
- Physical damage repair
- Ransomware demands
- Attack remediation
- Losses occurred

There are a few major caveats to that, however. A couple of factors may prevent the insurance company from paying out the plan. Some of those exceptions include poor security, human error, misconfigurations, insider attacks, and prior breaches. Some plans may cover legal fees, but will more than likely not cover regulatory fees from laws such as HIPAA and GDPR.

There should be policies in place for who needs to be contacted and when. Once unusual activity, be it by a monitoring tool or Security Operations Center, it should be immediately relayed to the Incident Response team. Once they receive notification and declare a breach, they must enact the IRP and notify management and the executive team. In addition to making sure all internal parties are informed correctly, the Communications Manager must also make sure the appropriate regulatory bodies are informed within the mandated timeframe, such as the HHS within 60 days if HIPAA is involved and the appropriate supervisory authority within 72 hours, if GDPR applies.

The last step of responding to a data breach is to learn from the incident. This is when you'll be doing a root cause analysis and audit logs to understand how it happened. If necessary, hiring a data forensics team can help get into the roots. Policies and procedures should be reviewed, updated, and tested after any major incident. CISA recommends running breach scenarios through tabletop or attack simulations. Following a breach would be the ideal time to make sure your revised policies will hold up. The lessons learned from this step should be used to help strengthen the prevention and detection

methods. This helps foster a system of continuous improvement and helps the organization stay protected from future threats.

Conclusion

Data breaches are a costly threat, regardless of size, and require careful, strategic planning to make the damages from them as minimal as possible. The landscape of threats is vast and constantly evolving. Rising threats from AI can pose serious risk to any company. The impacts from even a relatively small breach can be detrimental. It only takes one breach to cause enough damage to shut down an otherwise stable company. Implementing strong policies and best practices today is paramount for strength tomorrow.

References

Cambridge. “Understanding HIPAA and Its Role in Cybersecurity.” *Cambridge College of Healthcare & Technology*, Cambridge College of Healthcare and Technology, 6 Jan. 2025, www.cambridgehealth.edu/healthcare-cybersecurity-privacy/healthcare-cybersecurity-privacy-information/understanding-hipaa-and-its-role-in-cybersecurity/.

CISA. “Incident Response Plan (IRP) Basics.” *CISA.gov*.

CISA. “Use Strong Passwords.” *Www.cisa.gov*, CISA, www.cisa.gov/secure-our-world/use-strong-passwords.

Elgan, Mike. “Cybersecurity Skills Gap Contributes to Increased Average Breach Costs.” *Ibm.com*, 17 Oct. 2024, www.ibm.com/think/insights/cybersecurity-skills-gap-contributed-increase-average-breach-costs?utm_source=chatgpt.com. Accessed 30 Sept. 2025.

Embroker. “How Much Does Cyber Insurance Cost?” *Embroker*, 26 Aug. 2020, www.embroker.com/blog/cyber-insurance-cost/.

Faddom. “Third-Party Risk Management (TPRM): A Complete Guide.” *BlueVoyant*, 2025, www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide?page=1&utm. Accessed 1 Oct. 2025.

Federal Trade Commission. “Data Breach Response: A Guide for Business.” *Federal Trade Commission*, 2021, www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

Fortinet. “What Is Cyber Insurance? Policies, Services, and Coverage.” *Fortinet*, 2024, www.fortinet.com/resources/cyberglossary/cyber-insurance.

Hodge, Steven. “Continuous Learning and Training for Cybersecurity Excellence.” *CyberRiskInsight.com*, 23 Jan. 2025, www.cyberriskinsight.com/operations/continuous-learning-training-cybersecurity-excellence/?utm_source=chatgpt.com.

IBM. “Cost of a Data Breach Report 2025 the AI Oversight Gap Think Report.” 2025.

IBM. “What Is the NIST Cybersecurity Framework?” *Ibm.com*, 14 Oct. 2021, www.ibm.com/think/topics/nist.

ISC2. “ISC2 Cybersecurity Workforce Study: Demand Strong for Cloud Security and AI Skills While Workforce Gap Expands.” *Isc2.org*, 31 Oct. 2023, www.isc2.org/Insights/2023/10/ISC2-Cybersecurity-Workforce-Study-Demand-Strong-for-Cloud-and-AI-Skills-while-Workforce-Gap-Expands?queryID=54912dc457b108b9b7d8b1c01f0a6aa0&utm_source=chatgpt.com. Accessed 30 Sept. 2025.

Kalat, David. “Nervous System: The First Major Data Breach: 1984 | Insights | Berkeley Research Group.” *Www.thinkbrg.com*, 8 Dec. 2020, www.thinkbrg.com/insights/publications/kalat-first-major-data-breach/.

Kaspersky. “Companies to Increase IT Security Budgets up to 9% in the next Two Years.” */*, 26 Nov. 2024, www.kaspersky.com/about/press-releases/companies-to-increase-it-security-budgets-up-to-9-in-the-next-two-years?utm_source=chatgpt.com. Accessed 30 Sept. 2025.

Kosinski, Matthew . “What Is a Data Breach?” *IBM*, 24 May 2024, www.ibm.com/think/topics/data-breach.

Kosutic, Dejan. “What Is ISO 27001?” *Advisera*, 2024, advisera.com/27001academy/what-is-iso-27001/.

Martinez, John. “11 Identity & Access Management (IAM) Best Practices in 2022.” *Discover.strongdm.com*, 25 June 2025, www.strongdm.com/blog/iam-best-practices.

Palo Alto Networks. “What Is an Incident Response Plan and How to Get Started.” *Palo Alto Networks*, 2025, www.paloaltonetworks.com/cyberpedia/incident-response-plan.

Parsons, Lian. “Why Is Professional Development Important? - Professional & Executive Development | Harvard DCE.” *Professional & Executive Development | Harvard DCE*, 23 Aug. 2022, professional.dce.harvard.edu/blog/why-is-professional-development-important/#Where-to-Take-Professional-Development-Courses.

Rahmonbek, Komron. “35 Alarming Small Business Cybersecurity Statistics in 2022 | StrongDM.” *Discover.strongdm.com*, 22 Feb. 2023, www.strongdm.com/blog/small-business-cyber-security-statistics.

RSI Security. “What Are System Hardening Standards?” *RSI Security*, 27 Apr. 2022, blog.rsisecurity.com/what-are-system-hardening-standards/.

Skebaite, Aurelija. “The 20 Biggest Data Breaches in History | NordVPN.” *Nordvpn.com*, 28 June 2024, nordvpn.com/blog/biggest-data-breaches/.

TechInsurance. “Cyber Liability Insurance Cost | TechInsurance.” *Www.techinsurance.com*, 2 Apr. 2025, www.techinsurance.com/cyber-liability-insurance/cost.

Thies, Becca. “Breaking down the 2025 Verizon Data Breach Investigations Report.” *SpyCloud*, 30 Apr. 2025, spycloud.com/blog/verizon-2025-data-breach-report-insights/?utm_source=chatgpt.com.

Verizon. *2025 Data Breach Investigations Report 2025 Data Breach Investigations Report*. 2025.

Wolford, Ben. “What Is GDPR, the Eu’s New Data Protection Law?” *GDPR.EU*, 2025, gdpr.eu/what-is-gdpr/.