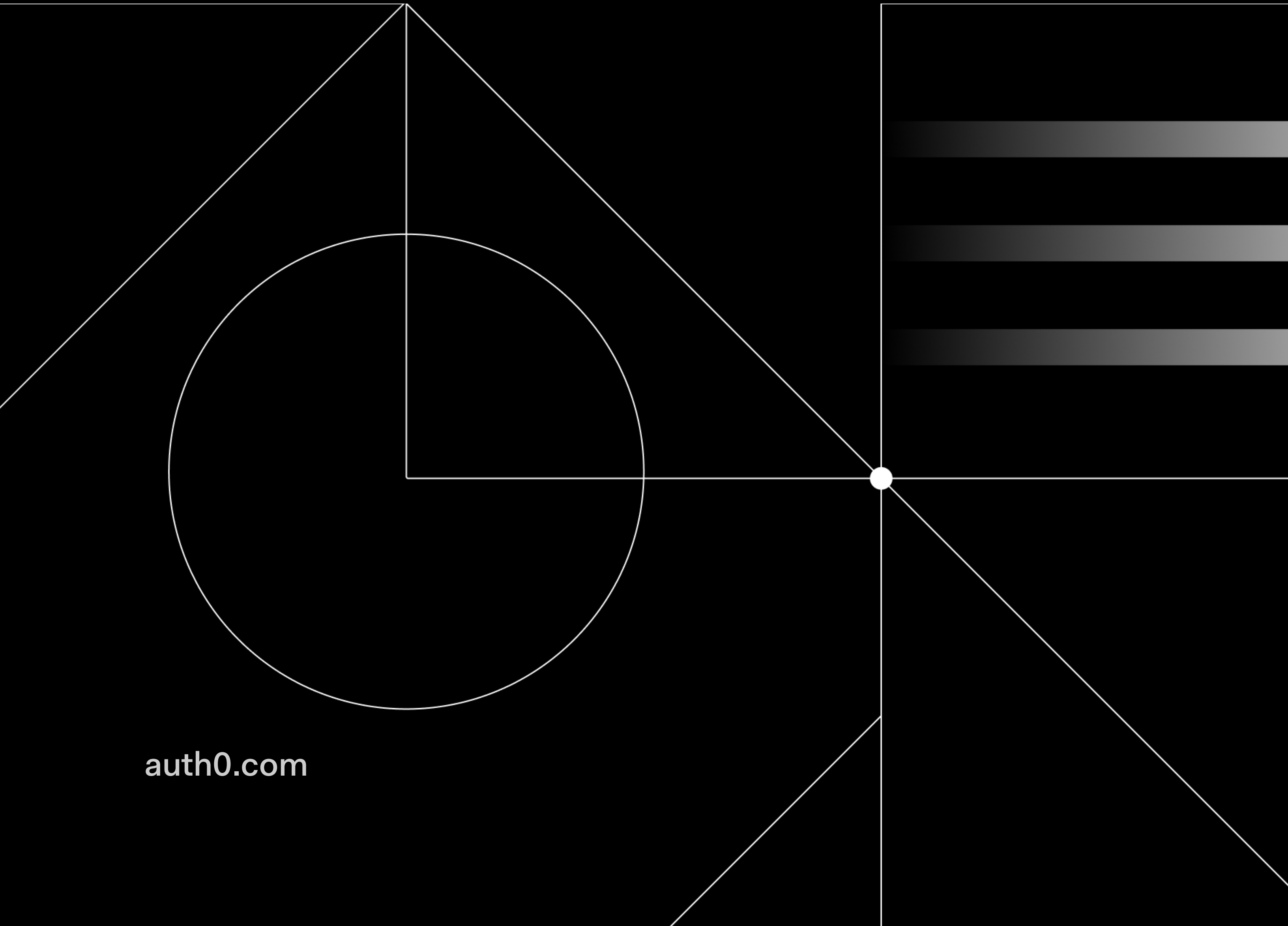
Auth0

How does a data breach impact your business?



auth0.com

How ready are you for a data breach?

Do we have your attention? Good.

We're not trying to scare you, nor do we want to lull you into a false sense of security. Rather we want to provide guidance as you bolster your breach defenses. The data breach numbers aren't encouraging (via the 2019 Cost of a Data Breach Report from IBM/Ponemon Institute):

- 27% — Global percent of companies that will suffer a data breach in the next 2 years
- 3.92M USD — Global average financial loss due to data breaches in 2019
- 8.19M USD — the average loss in the US for the same year
- $150 USD — average amount lost per customer record breached

This paper has one goal — to lay out the facts about how a data breach will impact your business. This includes ideas and suggestions for what you can do about it starting before the breach, extending through the event itself, and lasting all the way through the often long recovery process. We want your business to have the resiliency it needs to weather a data breach and come out intact, or possibly even thriving.

You'll see that word resiliency a lot. That's because it's an important concept in business today. It has also become somewhat of a buzzword, so to ensure we're all starting on the same page, in this paper we employ a broad definition so as to capture more behaviors under this umbrella term:

> A resilient business is one that has the intrinsic ability to regain a dynamically stable state in order to continue operations without losing its core purpose and values in the face of a dramatic turn of events.

So business system resilience means being prepared for the unknown. It means having processes in place that take into account the possibility of a breach, testing those processes, and being ready to put them into action should the moment arrive. This gives you the ability to mitigate first the likelihood of a breach (by minimizing your attack surface), then should one occur, the impact it has on your business (by remaining flexible and agile).

There is a stark internal divide when it comes to teams addressing data breaches and their impacts. In the same study by IBM, 61% of IT managers say they do not have faith in the company's ability to stop a potential breach, while 63% of CMOs say they are confident that the company can and will bounce back from the business impacts after a breach. These CMOs also tend to allocate substantially more of their budgets to brand protection than their CIO counterparts.

This divide appears to be based largely on the differing views from the two departments, combined with a lack of interaction between them. IT deals with infrastructure; the networks, computers, and users (internal employees) that make up the organization. While marketing looks at business processes, customer relationships, and the people outside the company that make up their target audience. These divergent viewpoints are one example of why it's crucial to bring stakeholders together and ensure they all get a holistic view of data protection and cybersecurity. Developing that holistic view starts well before any breaches occur by addressing the question, "how secure is your data, today?" and continues through the fallout after a breach when you'll need to rely on empathy and clear, concise communication.

This brings us back to our overarching topic, how a data breach can impact your business. In order to address that question, we're going to start with a look at the difference between data security and access control. From there we'll move on to a discussion of the top impacts a data breach can have and we'll wrap things up with a look at how to best handle the aftermath of a breach, should the worst-case scenario happen.

Securing Data

Digital transformation is a phrase that's been getting a lot of attention recently. It's also a phrase that seems to be widely misunderstood. Digital transformation of business and industry is an ongoing process, not a one-time upgrade. It's not the shift from paper to computer, that's digitization. Digital transformation is all about adaptability. Technology comes in waves and it's up to each company to decide which advances they adopt and which they pass over. That is digital transformation done right, adopting the technology that enables the company to thrive.

If you build your business infrastructure and processes to be adaptable, their flexibility is more likely to carry you farther into the future without breaking. You'll also be better positioned to weather the storm that is a data breach. You're setting yourself up to be one step closer to future-proof — that mythical status all organizations strive for. Adaptability is a theme you'll see several times in this paper. It's key to making business processes more resilient and able to pivot the company's direction to avoid disaster after a breach. The first step to building an adaptable business is to ensure that your data is secure. That also means you have the ability to track who is accessing what, when they're accessing it, and what they're doing with it.

Data security in a nutshell

Data security is a broad concept that encompasses an amalgamation of business process, procedures, and technologies that a company implements to ensure that prying eyes aren't looking at their data. According to IBM, who runs a yearly report on the business cost of a data breach, 51% of breaches in 2019 originated with an outside malicious attacker. At the same time, however, a full 40% were down to human error or system glitches. Adding to the confusion around root causes is the fact that 33% of reported breaches involve social engineering, so include both a malicious outsider and an internal, often unwitting, accomplice.

To cover this broad subject without overly simplifying it, we'll use the industry-standard CIA Triad (Confidentiality, Integrity, Availability). These three fundamental aspects underpin all information security frameworks, and when applied to your data security needs help to ensure that you cover all vectors.

Confidentiality

In data security, confidentiality means that information is not disclosed to unauthorized entities. Ways in which confidentiality can be compromised include everything from cyberattacks, laptop theft, a badly configured access control, or even just a misdirected email that sends the right information to the wrong person.

Integrity

Data integrity is the concept that your data must remain accurate and consistent throughout its entire lifecycle. Maintaining data integrity is a key component of any data security plan as all your business processes must be unpinned by trust in the quality of your data.

Availability

From many perspectives, data availability is the single most important aspect of the CIA Triad. In order for a company's data to be of value, it must be available. And ensuring the availability of digital assets is the sign of a robust IT infrastructure. This includes not only procuring the bandwidth to move it, the hardware to process it, and the server space to store it but also the ability to restore it if it's lost or corrupted.

To ensure these factors remain intact and their data is usable without exposing it to potential threats, businesses can select from myriad tactics and techniques. For the purposes of this paper, we're going to discuss the big three; regulatory compliance, redundancy, and encryption.

Regulatory compliance

Researchers and policymakers put years of work into the development of the GDPR, CCPA, PIPEDA, etc. The regulations they developed are comprehensive and were designed to be all-encompassing ways to keep your personal information private and secure.

Redundancy

More than just making sure the server backed up last night, data security relies on multiple types of redundancy. Yes, backups are still relevant, but now it's down to your cloud provider backing up your instance rather than the IT team backing up the on-prem servers to tape and transporting them off-site. Redundancy also applies to network infrastructure. We discussed availability as a major component of a robust data security model, and having a failover in the event of a network outage is crucial to keeping your data at the ready.

Encryption

In broad terms, encryption is the act of making information unreadable to anyone other than the intended audience. When it comes to disk encryption, this means only the systems or employees with access to the key can read the data stored on that disk, protecting you from physical attacks such as a stolen laptop. For transport encryption such as TLS, it's a matter of having a trust relationship established between entities so the receiver has the appropriate key to unlock the information sent, preventing eavesdropping during the communication.

Should a breach occur, and you can prove the data was encrypted at the time, your business can be released from potential liability as you are able to demonstrate that you took care to protect your data. Your customers will also appreciate that even though their data might be out in the wild somewhere, you had the foresight to ensure that it was unreadable.

Access control in a nutshell

Access control means not only stopping outside actors from getting their hands on your data, but also monitoring and controlling which internal stakeholders have access to what data. In Varonis Labs 2019 Global Data Risk study, it was found that 53% of companies had mission-critical data files that were accessible by every single employee, no matter their department or role. That's scary.

When it comes to implementing access control measures, a strong IAM, or Identity and Access Management, solution can offer several frameworks to choose from. These can be mixed and matched to some extent, but in the interest of manageability, it's best to stick with one overarching access model where possible.

When looking at overhauling existing access controls, there are three primary components to remember. These components will overlap to some extent, nevertheless, it's important to take them all into account individually when assessing an IAM solution. These components are Authentication, Authorization, and Management.

Authentication

Often mistaken for the entirety of access control, in reality, authentication is the first step wherein a system verifies the identity of the person or system requesting access, ensuring they are who they say they are. This is done via familiar steps such as entering a username and password or a biometric scan.

Authorization

Once authenticated, a user account must have rights and privileges associated with it. These determine what resources can be accessed by that account. The access level can include everything from application privileges, read rights to a certain database, or edit rights for an individual file. Dovetailing from this is the ability to audit existing accounts to maintain proper access levels and rights. This is the principle of least privilege in action, ensuring that people have access to everything they need, and nothing more.

Management

Crucial to maintaining security is the ability for administrators to remove depreciated accounts, reassign rights for employees who change roles, etc. A solid IAM solution can connect to your existing user database to streamline this process and ensure each change is replicated to the right resources. The logs created can then be used to audit activity so you are able to hold a user or a system accountable for their actions.

As you can see, access control is but one aspect of a sound data security plan, albeit a crucial one. We would be remiss if we didn't give a mention to one additional piece of the data security puzzle — user training. The fact that ⅓ of data breaches involve social engineering is a telling statistic. Employee training is one of the, if not the single, most under-funded aspect of cybersecurity. To make a dent in the impact of these attacks, your employees need to understand what a phishing email looks like, how to determine the efficacy of chat messages they receive, and even what to look out for when entering the building to avoid piggy-backing. Pair that with a clear SOP document that lays out who to report suspicious activity to and you're well on your way to curbing the potential data breaches that can result from social engineering tactics.

The Top 5 Impacts a Data Breach Will Have on Your Business

We hate to be the ones to break it to you, but no matter how tightly you lock down your company's proprietary data, there is still that 1 in 3 chance (IBM/Ponemon) that you will be the victim of a data breach in the next two years. While data privacy regulations have reporting requirements (ex: 72 hours under GDPR), the true extent of the damage may not be known for some time, as it takes, on average, 279 days to identify a breach, and 73 days to contain it (IBM/Ponemon). By knowing ahead of time what damages and impacts you're likely to see, you will be better positioned to emerge on the other side of a breach a stronger business entity with happier customers and more privacy-aware employees.

1. Financial costs

Even if your company is not headquartered in the EU, or California, or anywhere else that is subject to data privacy regulations, chances are you have customers who are so you need to be compliant. This also means that you're subject to fines and penalties as laid out in the GDPR, CCPA, etc. Beyond that, you're looking at the potential for legal fees if personally identifiable information (PII) was involved.

If you're a publicly-traded company, your stock will take a hit. Ponemon Institute's Impact of Data Breaches Report showed an average 5% drop upon public notification of a breach. However, it also showed that with a strong pre-breach security posture the drop can be mitigated and turned into a lower, if slightly longer curve to recovery.

2. Brand reputation

Nearly a third of customers whose data was leaked discontinued business with the breached company. People value their privacy and put their trust in companies every day. They trust that their information will be treated with respect and kept private. The betrayal felt when a data breach happens is real and needs to be handled by the company in a way that shows empathy, care, and respect. How you respond to a breach will define your brand reputation for years to come.

3. Business disruption

Business resilience includes having a strong business continuity plan (BCP) and an Incident Response (IR) plan in place. The IR plan must include what to do in the event of a data breach as this will involve working with multiple stakeholders from (at least) IT, Security, Customer Support and Legal. To pull an example from recent events, a major healthcare provider with locations on two continents was hit with a ransomware attack. While they determined the full extent of the attack, what data was accessed, if anything was stolen, etc. the IT security team had to completely shut down the network across their North American operations. That left people using pen and paper to update patient records, write prescriptions, etc. Fortunately, they were able to divert critical cases to other facilities and no lives were lost, but the impact will be felt for some time.

4. Lost customer trust

We talked about the loss of brand reputation that can occur in the wake of a breach. There's another piece of that impact that we want to cover as well, the loss of trust that can lead to an increase in customer churn. Ponemon Institute's Impact of Data Breaches Report, cited above, showed that of the 51% of consumers who had been involved in a breach over the past two years, 65% lost trust in the business. That's a deeper impact than the 27% who discontinued doing business with the company.

Conversely, a full 65% of consumers say they will make more purchases from a company they trust, as they feel an increased sense of loyalty to these brands for treating them well. And of those, a staggering 75% say they'll recommend these businesses to friends and family. And since people trust people, those referred are also more likely to make purchases.

5. Data loss

No list of business impacts would be complete without mention of the data itself. No matter the root cause or full extent of the breach, if data was touched there will be an impact on the business. If it was customer information that was leaked to bad actors, the impact is public-facing and will take a fair amount of time and resources to clean up and recover from. If it was proprietary company data, say an outside attack aimed at your R&D department, that team will now spend even more time and resources trying to recover the work lost, recreate the data points, etc.

Controlling the Aftermath of a Breach

In the wake of a data breach, a business will face much scrutiny. Their customers will be waiting to hear if their data was compromised, investors, along with the public, want to know if their stock price is going to rebound, and regulators will be examining what rules may have been broken. Inside the organization, Infosec will be working to contain and recover from the incident, legal will be working out the ramifications for the company, and PR will be working to reduce the impact to the company's brand.

Really you will be judged on whether you paid attention to your data security and did not make any indefensible errors or lapses of judgement. And, you will be judged on how you respond. How you manage the aftermath and how you communicate with your customers.

That's a lot for anyone to manage, yet it is to that management that we now turn. As has been mentioned already, brand reputation, customer loyalty, and organizational trust are all integral to business resilience in the days, weeks, months, and even years following a data breach. Communication is a priority, as is damage control, root cause analysis, and tightening existing security measures.

Determining the root cause

As part of that root cause analysis, you'll likely find that the breach originated from one of three places: an outside malicious actor, an insider (whether malicious or accidental), or a system error/glitch. More than likely, you'll find some combination of these at play.

Malicious actor

Businesses of all sizes can find themselves the target of a malicious attack. These can originate with everything from a phishing scam, to ransomware, to a direct SQL injection attack. In many cases, several vectors are used in tandem to effect a breach.

Insider threat

In most cases where a breach involves an employee, their part was as an unwitting accomplice rather than an active attacker. That said, the former is no less worthy of sustained attention in the follow-up period. Education is step one. Train employees to better identify threats like phishing emails, social engineering phone calls, and malicious email attachments.

System error/glitch

In terms of data breaches, the most prevalent glitch involves broken authentication like compromised passwords. Many log-in systems don't include a built-in way to ensure that users aren't recycling passwords, or enforce the regular changing of existing ones. Creating a strong employee password protocol can go a long way toward eliminating future breaches due to mismanagement of user accounts or passwords.

Best practices to contain data breach fallout

There are many ways a breach can proceed between origination and discovery. What will not change, however, is a set of best practices you can follow in the days following discovery to limit the overall business impact.

Be prepared

Have a plan and make sure you have tested that plan with all stakeholders. Understanding with whom and how you will need to communicate will be critical to managing the post-breach scenario.

Be transparent

Starting well before any breach occurs, talk to your customers about the steps you're taking to keep their private information secure. Tell them what information you keep, why you keep it, and what you do with it. Not only is this a requirement under many data privacy regulations but by being open and honest with your customers during the peaceful times they'll be far more understanding and loyal should things go sideways later on. When you experience a breach, talk to those affected, be empathetic, and let them know truthfully what's going on. And down the road, keep everyone updated on additional steps being taken and reassure them that you're doing everything in your power to prevent another such occurrence.

Be concise

At the same time, don't divulge too much. While transparency is a good thing, it can be taken too far when companies share details about how a breach occurred or give out details of internal data that was part of the breach. Keep statements brief and succinct, only telling those involved of the nature of the data exposed while giving everyone else the 10,000-foot view.

Own it

Own up to the fact that a breach happened. Don't try to pass blame or say it was "unavoidable." The truth does wonders for quelling unrest among employees, customers, and the public. It also shows your human side, and people connect with people better than they do with faceless brand names.

Conduct a full audit

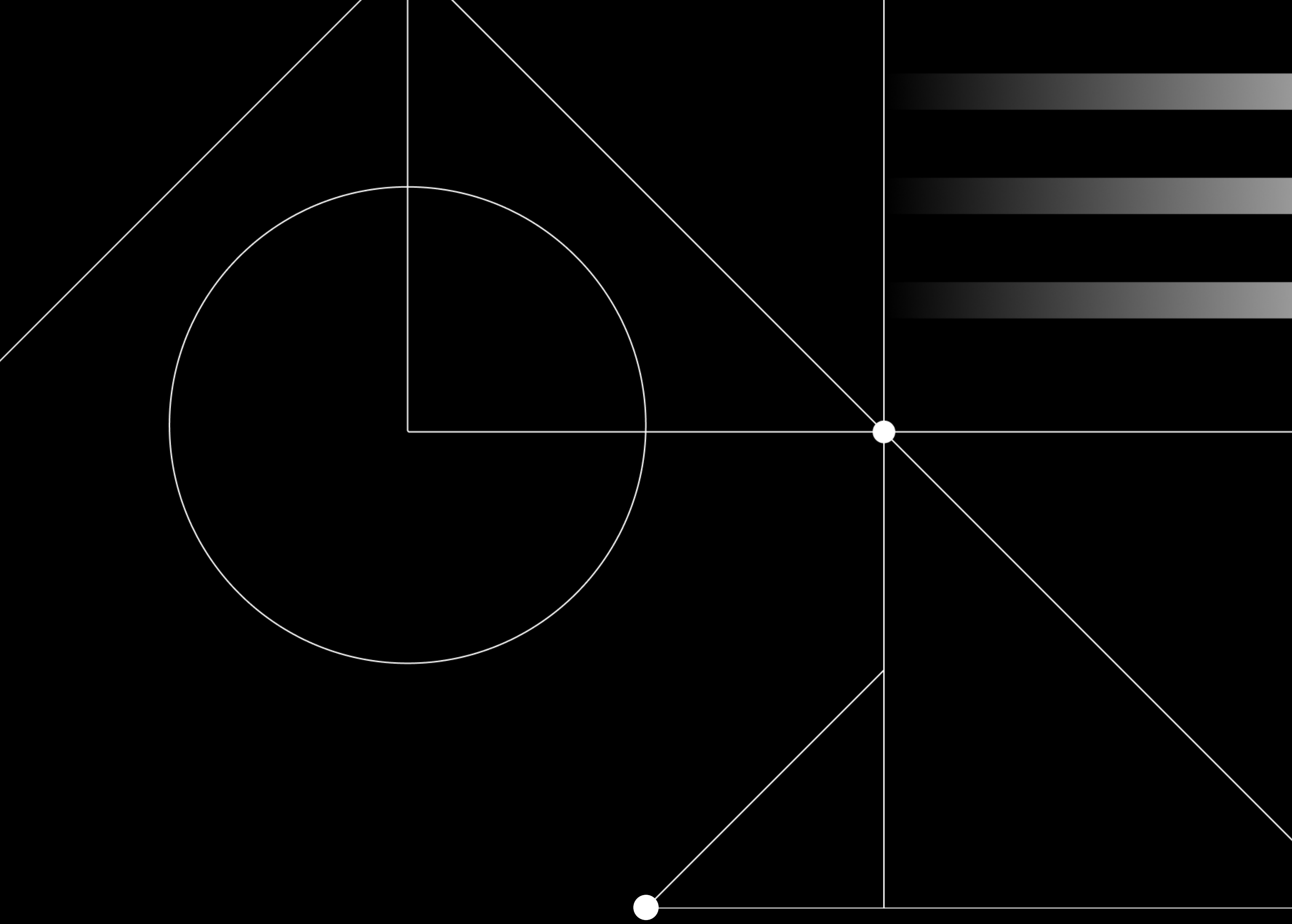
Immediately following the discovery of a data breach, begin analysis. You need to get to the root cause as quickly as possible so you can do two things: stop the outflow of data and alert those involved. Consider bringing in outside security specialists to assist. Your team is no doubt top-notch, but having an expert on your side can help immensely when it comes time to talk to those involved.

Shore up your defenses

Once the results of that audit are known, it's time to build up your defenses. Reports show that the stronger a business's security posture is, the shorter their overall recovery will be, and the lower the total cost.

Are You Ready for a Data Breach?

It's in your best interest to stay out front when it comes to the specter of a data breach. By communicating clearly, concisely, and transparently with your customers starting today you can do just that. And by taking steps to strengthen your security posture now, things like implementing strong IAM procedures, developing a robust business continuity plan, and ensuring your incident response team is trained and ready — you can greatly improve the likelihood of avoiding a breach altogether. Auth0 can help with the IAM, so reach out to our experts today to begin the conversation.



Auth0

About Auth0

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit www.auth0.com or follow @auth0 on Twitter.