1Password

GUIDE

Incident response guide

What to do if you experience a breach

Introduction

Data breaches can affect any business at any time, whether you're a scrappy startup or an enterprise juggernaut. With cyber attacks surging, and the tactics behind them rapidly evolving, protecting your business can feel like a never-ending game of cat and mouse. And considering the risks to your business – and your customers – it's not a game you want to lose.

Most breaches are preventable, if you implement some basic tools and habits across your workforce. But when security incidents do happen, a fast, calm, and systematic response from your team could mean all the difference. With the right people and processes in place – and a clear, comprehensive incident response playbook – you can minimize the repercussions and offer peace of mind to your customers, employees, and investors.

In this guide, we'll walk you through some major considerations for responding to a data breach. No two incident response strategies are created equal; you'll need to cater your approach to your business's specific needs, and continue to update your plan as your company grows and threats evolve. These suggestions can hopefully offer a framework of ideas as you get started!

People, processes, and playbook

Let’s back it up: Well before a potential incident happens, there should be a good deal of planning and prevention. And just like there isn’t one perfect incident response playbook, there is no single, out-of-the-box toolkit for proactive measures against cyber attacks. Much depends on your company’s environment, goals, budget, and so on. But there are some guiding principles you can follow to prevent a breach, including being prepared to respond if one happens.

Whatever the specifics, your preparation should involve some combination of people and processes, along with well-thought-out documentation in the form of an incident response playbook. And it’s never too early to get moving.

67% **of U.S. small businesses don’t have an incident response plan in place.**

VentureBeat

“Any company of any size is vulnerable, and a major mistake most startups make is not having security in place from day one,” says the 1Password Security team. “This creates an unsustainable level of tech debt that must eventually be caught up on. But at the point most companies think to bring in security, it’s too late and the new team is overwhelmed just doing daily firefighting. If you plan this stuff from the get-go, it’s much easier overall.”

“This is really indicative of a larger issue in the industry: looking at Security teams as cost centers with some unrealized ROI. Security doesn’t exist to make the company money. Security exists to prevent the loss of massive sums in a hack, or related fines and sanctions, or from loss of consumer confidence and revenue.”

> **Security doesn’t exist to make the company money. Security exists to prevent the loss of massive sums in a hack, or related fines and sanctions, or from loss of consumer confidence and revenue.**
>
> - 1Password Security team

Starting from zero can be a challenge, but waiting for something bad to happen before you get started is a risk you can’t afford. If your in-house team doesn’t have the capacity, consider hiring an outside cybersecurity consultant to help identify your biggest vulnerabilities and recommend the right actions to put in place. You might also consider enlisting some external agencies to assist your team with certain aspects of incident response – such as managed detection and response providers. That said, hiring and training in-house experts, sooner rather than later, will offer the most holistic coverage and reap lasting benefits.

“Internal deep knowledge will always be more useful and successfully utilized than a consultant coming in every few months. Invest in your people, invest in your talent,” says the 1Password security team.

In your budgeting and team planning process, prioritize hiring an experienced DFIR manager (Digital Forensics and Incident Response) or building out a training program to promote an employee into the role. Empower them to make the tough decisions about your DFIR strategy, including team structure and priorities, along with the technology they might use for different facets of incident response.

“If you don’t have this experience in-house, hire ASAP,” the 1Password Security team advises. “DFIR is a specialized skill set drawing an experience from many facets of technology, including generalized security experience, penetration testing, Ops/DevOps experience, development skills, and more. You simply can’t just expect non-specialized personnel to handle a role like this. And if you want to build up someone internally who already has an interest in this work, the best thing you can do is hire them a mentor.”

Read our **data breach prevention checklist** on how to prepare for potential security incidents, as well as our guide on **how to avoid a data breach** to minimize your chances of a major incident impacting your business.

Playbook basics

Deciding your exact incident response plan should be a labor of love and careful thought. Focus on what resources you have (or don't have) and identify their impact, as well as how different types of attacks would affect your data, customers, systems, etc. Your step-by-step response will be built around those factors.

Generally, the stages of incident response follow some variation of this formula:

1. **Identification**
2. **Triage**
3. **Response and notification**
4. **Post-mortem**
5. **Future planning and preventative work**

Even within this framework, the particular subtasks or action items will vary based on the incident details, the data or people affected, your IT infrastructure, and more. But fast, thorough action is a must to minimize risk for your business and customers alike.

Once your Security team assembles a playbook – that addresses the exact actions to take in a breach with respect to your tools and team structure – it should be made available to your entire workforce.

"Everyone should understand and have access to the basics of the playbook," says the 1Password Security team. "Store it wherever employees can access it quickly and easily. It should be as simple to find as the employee handbook."

In the following sections, you'll find brief overviews of these common incident response stages. Some version of this approach is becoming standard practice for how businesses handle these objectives – no matter their industry – to limit the cost and consequences of data breaches, and prevent similar incidents from happening down the road.

Identification

First things first: You can’t solve a problem that you don’t know exists. And you can’t repair damage you don’t know the extent of. By investigating red flags as they come up, your incident response team can get a sense of what happened and determine the appropriate response. In short, gathering the “who, what, when, where, and why” of any incident, in as short a time as possible, is absolutely vital.

Ways of identifying a breach can include:

- Notifications from cybersecurity software or IT monitoring tools.
- Abnormalities in routine audits (ex. server, network, or data).
- Unusual traffic or unapproved activity.
- Reports of suspicious information on your website.
- Reports of system failure or performance issues from employees.
- Employees reporting their security oversights or mistakes.

Employees and visitors alike can be major (and often unexpected) allies in the incident identification phase, with concerning observations they report. By making it easy for them to contact your IT/Support team if they see something suspicious, you improve your chances of problems being detected early.

Deploying some monitoring tools of your own should also be a high priority. These platforms may pull from different sets of data or activity sources across your business, or have different alerts set up. Choosing the right tools will depend on your scope and the technology you already use. Some free and open-source options exist as a potential starting point, but as you scale, your team may want to consider paid-for solutions.

Once your team’s red flags go up, whatever the source, they’ll need to complete thorough reviews of your databases and activity logs. This forensics process should identify what triggered the incident and its reach across your infrastructure. If any affected servers or hardware are still online, they should be taken offline until forensics and remediation is complete.

It’s a common misconception that breaches will set off red flags as soon as they happen. Many cyber attacks creep into business servers and linger there for weeks, months, or years – slowly and stealthily copying or infecting data.

When it comes to cybersecurity threats, the candle is unfortunately burning at both ends: The average business still has limited or no DFIR resources, and attacks are growing more sophisticated each day – often flying under the radar and costing more the longer they go undetected. This is a major reason why **DFIR is no longer the luxury that it used to be, but rather a critical “keeping the lights on” cost.**

Identify when company or employee accounts are compromised in a breach with 1Password’s **domain breach reports**, **Watchtower**, and **Insights dashboard**.

“As mentioned before, simply considering the upfront costs of personnel and tools when it comes to DFIR is shortsighted; **DFIR exists to prevent extreme loss**,” says the 1Password Security team. “Another thing to remember, most of their work is not visible on a day-to-day basis. Your DFIR team is most successful when you don’t realize they’re doing anything at all most days; it means you’ve not been breached. In other words, **no news is good news.”**

250 hours

how long cyber criminals often spend in networks undetected.

TechRadar

287 days

the average time it takes businesses to detect and contain an attack.

VentureBeat

IBM reports that those teams who can contain a cyber attack within 30 days save an average of $1 million in losses. Researching and testing out an effective identification process is clearly worth the effort. You’ll also need to reevaluate and optimize your plan as your business – and the threat landscape – continue to evolve.

Triage

With the suspected incidents now identified, your DFIR team needs to then:

1. **Verify their legitimacy**
2. **Determine the steps for analysis and remediation, along with the people they'll need to contact**
3. **Prioritize next steps based on urgency**
4. **Perform the most critical actions before planning out the rest**

This process is often referred to as triage, after the term used in hospitals for urgent care. Your team's findings here will inform their next actions, which will also vary based on the type of incident, your company structure, and how many people were (or might still be) affected.

The Insider's Guide to Incident Response from AT&T summarizes some of the more prevalent attack types and the suggested top-level actions. But naturally, your exact response, prioritization, and if/when to go public about your incident should be determined by your Security/DFIR team. Part of their routine duties is to stay informed about emerging threats, how those threats might affect you, and what the best response would be for varying events. The more proactive work done here, the less that will need to be done when incidents occur and time is most precious.

After the compromise has been mitigated, a key response item is updating credentials for any account or system that's been compromised. A company-wide password manager like 1Password can help employees make these changes quickly and with little stress. Features like 1Password's domain breach reports help IT and Security teams identify all the potentially compromised accounts after a breach, and make it easier to request those users update their information.

Getting the triage process right is a delicate but essential task, and will be a test of your DFIR team's knowledge, collaborative abilities, and problem-solving skills. Once it's confidently laid out – or as confidently as it can be – they can proceed with their determined actions and communicate relevant details with those that need to hear them.

Response and notification

Your Incident Response team – along with any external support they need to loop in – will need to procedurally eliminate the threats they've identified, while closing the gaps and vulnerabilities that the attackers took advantage of. This may include updates to all the affected accounts or endpoints, installing security patches where needed, restricting access to certain networks or applications, or removing certain apps, servers, or hardware from the company's infrastructure entirely. In the process, your team will repair, remediate, and reinforce the affected data wherever possible.

Certainty is key when resolving a security incident. This entails testing the response, executing the actual response once it's been tested, and validating that the issue has really been resolved – and won't repeat itself. "You can say you've done it," says the 1Password Security team, "but you also have to prove it's been done."

Then comes the extremely sensitive step of notification, if the situation calls for it. Depending on the extent of the attack and volume of people and data affected, this may involve messaging to your extended workforce, your active or past customers, your investors and business partners, and – in the most significant cases – the public.

Minor internal incidents that don't pose any wider threats may not require this step. But if your team determines a need for broader communication, they should connect with some combination of HR, PR, and Legal teams to craft the messaging, determine the right channels, and prepare for the potential response.

You only get one shot to get this messaging right. Due to the costly nature of some attacks and their ramifications around employee and customer safety and privacy – not to mention your brand trust and financial future – every detail matters. As do the methods of delivery.

Along with the official messaging you craft for these different audiences, make sure your broader workforce knows what to say (and what not to say) when approached about the incident. They should also know where customer inquiries should be directed, and to not casually discuss these confidential details with people outside of work.

Post-mortem

Let’s say that – fingers crossed, knock on wood, etc. – your team has successfully resolved the security issues, closed the gaps, and communicated the situation. Let out a sign of relief. But then get back to it – there’s still work to do.

Post-incident analysis and documentation is essential while the event is still fresh, to accurately log the event details and the response taken. This post-mortem process (or post-incident review process) will create a valuable repository for later reference and help capture any potential takeaways – for both shaping your future incident response and improving your business operations as a whole. Insights like these will help the team safeguard your data, company, and customers heading into the future.

The post-mortem process will create a valuable repository for later reference and help capture any potential takeaways.

As with your other DFIR processes, much will depend here on your team structure and technology. Sometimes it’s just a document; other times it might require a conference with the parties involved or various stakeholders. At the very least, each incident should be summarized in a report that includes a timeline of the incident, customer impact, who was involved, and other relevant details. This can be manually drafted or produced with the help of pre-built templates, and stored in an encrypted folder or in an incident management tool.

There are additional tools like digital forensics or timeline analysis software that can help your DFIR team gather findings and draw outcomes from a security incident. As with other stages in incident response, there are different paths you can take depending on your needs, budget, etc. Your in-house experts can decide what suits them, and reference some trusted online sources for help with writing incident post-mortems and keeping up with best practices.

Future planning

With the incident done and documented, your DFIR team should act fast on the learning opportunities it illuminated for them. “From the post-mortem you have key insights, new goals for prevention, and so on. Future planning is basically taking that and going with it – taking remediatory steps from the post-mortem and putting them into practice,” says the 1Password Security team. “If you notice a flaw in the way something works, how a notification failed, any communication issues. That’s something you need to plan to act on. And sometimes it won’t get done right away; depending on the scope, it might be an ongoing project.”

Some examples of DFIR preventive work:

- Updating team, company, or customer policy.
- Adding, removing, or adjusting measures in different incident response plans.
- Research into aspects of past incidents, emerging threats, DFIR technology, or industry news.
- Process or system optimization.
- Implementing security training for your team.

Your incident response playbook should be assessed and updated annually, at minimum. A tabletop exercise is an affordable, effective way to evaluate what updates you should make. The threat landscape never stops changing; you need to keep up to date in order to keep your business and customers protected. The best preventative work you can do as a company is creating or continuing to invest in a dedicated team that can steer DFIR initiatives, focus on your company’s preparedness, and be ready when the time calls. Even a one-person incident response department will be a massive leap for your business in catching and mitigating the risks of security threats.

Move forward, together

Human-centric security is not a buzzword. It’s an important (and overdue) perspective shift about cybersecurity. The single most important step in preventing cyber attacks is protecting your people. This requires education about online security, transparency and support for your IT team, and providing tools that help faster safer habits.

82%

of data breaches are traced back to a human element like weak or reused passwords.

Verizon

A password manager makes the secure way of working also the easiest. It helps with creating, safe storing, and secure sharing of passwords and other details for all their apps and accounts. Since most data breaches are traced back to your humans – and behaviors like weak, reused, and misused passwords – it can help you and your Security teams address your single biggest vulnerability.

Paired with proper training and broader awareness of online threats, password management makes your entire workforce active contributors to your security strategy.

Try 1Password Business free for 14 days, and see why more than 100,000 global businesses trust 1Password with their most sensitive data.

Read more about the **benefits and importance of a password manager for your business**, and how you can create a **culture of security** that empowers your employees to do their part, and makes security “an everyone thing” – not just “an IT thing.”