kaspersky

Your guide to setting up a cybersecurity incident response plan

kaspersky

Contents

Heavy numbers

According to a 2021 survey carried out by VMware in partnership with Kroll, Red Canary and Wakefield Research, the vast majority (93%) of organizations had suffered a cybersecurity incident in the past 12 months, while only 49% said they felt equipped (in terms of tools, staff and expertise) to detect or respond to cyber threats.[1]

What is a cybersecurity incident response plan?

A cybersecurity incident response plan (CSIRP) is a document that tells you and your staff what to do in case of a security incident such as a data breach, ransomware attack, service outage or loss of sensitive information. The incident plan has several steps, including identifying incidents, recognizing their priority, containing and eliminating them, recovery, and taking actions to prevent future incidents. The plan also includes roles and responsibilities—that is, who in your company does what in the event of a security incident—and communication plans. We'll be covering all of these elements in this guide.

The National Institute of Standards and Technology (NIST) has a complete guide to setting up a CSIRP, which you can find here. It's a little bit lengthy and detailed — that's why we've extracted the best bits for you here!

[1] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-state-of-incident-response-2021.pdf

The cost of a security breach

No company which is storing or processing sensitive data is small or secure enough to completely avoid security breaches, in any industry.

- The Ponemon Institute's 2020 Cost of Cyber Crime study found that the typical organization experiences 130 security incidents per year[2]
- The cost of cybercrime is predicted to reach USD 10.5 trillion by 2025, according to the latest version of the Cisco/Cybersecurity Ventures "2022 Cybersecurity Almanac.[3]
- According to IBM's annual Cost of Data Breach Report 2021, the average cost of a data breach was the highest in the 17-year history of the report at USD 4.37 million.[4]
- The same report found that the average cost of breaches where remote work was a factor in the breach was USD 1.07 million higher (compared to breaches not involving remote work), meaning that the tendency to shift to remote work patterns following COVID-19 has significantly contributed to the cost of data breaches.
- Another survey conducted by the Ponemon Institute found that 77% of businesses in 2019 did not have a security incident response plan in place,[5] leaving them wide open to a costly security breach.

Talking the talk but not walking the walk

In 2015, telecoms company TalkTalk was fine a record-breaking £400,000 by the Information Commissioner's Office (ICO) following a massive customer data breach. That fine could have been as large as £60 million if the maximum penalty had been applied. The ICO's investigation[6] found that the breach could have been avoided if some simple steps had been taken, like regularly updating their systems and proactively monitoring threats — basic elements of a good incident response plan. If the company had had a robust CSIRP in place and their staff were well drilled in it, a huge cost and reputational damage could have been saved.

The Human Factor

Cyber attacks have a human cost as well. For example, the Kaspersky Global Corporate IT Security Risks Survey (ITSRS) 2019 found that 33% of staff felt much more stressed at work as a result of a data breach, while 30% had to miss out on an important family event or personal date because they were working late after a data breach. Read the whole survey here.

A fault in the pipeline

The May 2021 cyberattack on the Colonial Pipeline, which carries oil across the United States, is another example of the kind of dangers that businesses face in the modern environment. The company paid $4.4 million in ransom to get their systems running again, apparently all just because their user login credentials had not been updated and strengthened[7] (a regular part of a CSIRP). Following the attack, US President Joe Biden signed an executive order to improve federal cybersecurity, noting that agencies need to "lead by example" —just another sign of the world that we're all moving into. Cybersecurity needs to be a top priority for all organizations.

For more about the current ransomware environment, check out this webinar.

[2] https://www.accenture.com/us-en/insights/security/eighth-annual-cost-cybercrime-study

[3] https://cybersecurityventures.com/cybersecurity-almanac-2022/

[4] https://www.ibm.com/security/data-breach

[5] https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

[6] https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/

[7] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Why do you need a cybersecurity incident response plan?

Stay cool in an emergency

If you don't have an incident response plan in place already, your security and management teams will be running around like crazy at the last moment trying to handle an emergency incident. They are likely to communicate poorly and act inefficiently, making the data breach much more costly than it needs to be.

Keep costs down

Regulatory fines, compensating customers, and investigating and recovering from incidents make breaches potentially very costly. A solid CSIRP will reduce all of these costs, making it a sound investment.

Stay in the good books

Some data privacy regulatory bodies (such as the California Consumer Protection Act) legally require organizations operating in their jurisdiction to have an incident response plan in place. Additionally, for certain industry-led security frameworks, like ISO 27001 certification, without an incident response plan you won't pass the audit to receive the certification.

Don't miss anything

If you experience a data breach, you might be legally required to take certain steps and notify the relevant authorities such as government agencies, as well as the affected parties. Without a CSIRP in place, you're likely to miss crucial steps or overlook such details, which will put you at risk of additional fines and legal action.

Cover all your bases

Following a significant breach, you will have to go through an external investigation or audit. If you can't provide evidence of having a CSIRP, the auditors will see that you aren't taking your responsibility for your sensitive data seriously enough and can impose stricter punishments. Furthermore, without a CSIRP your insurance premiums are likely to be considerably higher, or your insurance could even be void! Ouch!

Rapid response and data protection

A good CSIRP includes detailed procedures for securing backups, ensuring secure identity and access management, and responding quickly to vulnerabilities and threats. Having these procedures already in place ensures your ability to rapidly resolve any incidents, protecting your data and systems.

Protect your reputation

Your customers are likely to respond very negatively if their data is compromised. Likewise, shareholders and investors may withdraw their support from a business that experiences a breach. On the other hand, responding effectively to incidents demonstrates your commitment to security and privacy, bolstering customer and shareholder loyalty and trust. In business, reputation is everything.

6 phases of a solid CSIRP

1. Preparation

The preparation phase is in many ways the most important section, as it provides the foundation for the rest of the plan. Technically, you should always be in the preparation phase: prepared for any emerging incident, and keeping your plan constantly up-to-date and operational. The key elements that should be included in the preparation phase are:

- Ensuring that all your employees are properly educated regarding data security and responding to cyber threats and emergencies.
- Conduct a risk assessment to prioritize security issues, identify the most sensitive assets and the most critical security incidents your team should focus on.
- Conduct regular training and drills so that everybody is ready to act appropriately in case of an incident. Check out page 10 for more on common incident plan drills.
- Assign the relevant roles and responsibilities for your cyber security incident team, and ensure they have access to the necessary systems and tools. For more information on team responsibilities, see page 9.
- Clarify the processes and lines of communication in the event of an incident. Who needs to be contacted, and when? Not having clear, established communications in an emergency can cause a lot of mess and inefficiency.
- Make sure that every aspect of your plan (training, execution, resources etc.) is approved, funded and available in advance. In short, is your plan operational?

Is the preparation phase of your plan complete? Ask yourself these questions to check:

1. Has everyone been trained on the necessary security policies and procedures?
2. Has your security plan been approved by management? Is it up-to-date and resourced?
3. Does everyone on the incident response team know their roles and action plan?
4. Has everyone participated in mock drills? Are they ready to respond?

2. Identification

This phase of the plan is triggered when an incident has just occurred, and you need to diagnose it and decide the appropriate course of action. You can't prepare specifically for all possible incident sources because there are too many, but your team should be able to effectively detect the type and severity of the threat and determine the response.

There are two types of sign that your security systems are under attack: **precursors** (detected before an attack happens) or **indicators** (detected during or after an attack).

- An example of a precursor would be a high number of failed login attempts, suggesting that an attacker is trying to penetrate your network by guessing a username and password.
- An example of an indicator would be an antivirus software alerting you that someone on your network has clicked on a malware link and their computer is infected.

This phase also includes **documentation**: your team should record everything that happens, including the nature of the attack, any evidence, and their actions taken to respond. This will be useful in the post-incident activities phase, in court and when facing the auditors.

Finally, this phase should also include **notification**: making sure that all relevant parties (law enforcement, federal agencies, customers, shareholders and affected businesses) are made aware that an attack has taken place. Timely notification ensures you stay on the right side of the law, protects your reputation and reduces your liability in the long-run. Your plan should include clear instructions on who should be notified and the steps in the notification procedure

Questions to ask at the identification phase:

1. When and where did the incident start?
2. Who discovered it, and how?
3. What is the extent of the compromise? Which areas are affected?
4. Are business operations affected? How?

3. Containment

When you first discover a breach, you might be tempted to just delete all the contaminated data as soon as possible to remove the threat. However, this would also remove all the valuable evidence you can use in post-incident audits, and to help you determine how the breach started and how to prevent it happening again.

Instead, it's better to contain the breach by disconnecting affected devices from the Internet, preventing any further damage to your business. It's also a good idea to have a redundant system back-up at the ready to help restore operations and not lose compromised data forever.

Containment can take two forms:

- **Short-term containment:** temporary solutions such as isolating the affected network segment, taking down any servers that have been compromised, and redirecting traffic to backup servers.
- **Long-term containment:** continuing operations using temporary solutions while rebuilding clean systems, preparing to bring them back online in the recovery stage.

During this phase you can also update and patch your systems, check your remote access protocols, change all system access credentials, and strengthen your passwords.

Prevention is better than cure

It takes an average of 287 days for a security team to identify and contain a data breach, according to IBM's Cost of a Data Breach report 2021.[9] That's why the preparation phase is so important—to prevent any incidents occurring in the first place.

There are a number of factors you should take into consideration when deciding on a containment procedure. The NIST lists them as follows:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., an emergency workaround to be removed in four hours, a temporary workaround to be removed in two weeks, permanent solution).

Questions to ask at the containment phase:

1. What are you doing to contain the breach in the short- and long-term?
2. Have you quarantined all affected areas?
3. What backups do you have in place?
4. Have all access credentials been changed and strengthened?
5. Have you applied all the latest security patches and updates?

4. Eradication

The exact steps in the eradication phase will depend on the type of attack you are experiencing. For example, you could be deleting malware, disabling any compromised accounts, closing vulnerabilities in the network, etc. Fundamentally, eradication means finding the root cause of the attack and getting rid of it!

Your team could be eliminating the threat themselves, or you could get a third-party to do it; either way, there's one important point to remember: the eradication must be complete. If even a trace of malware or affected areas remain in your systems, you could still be suffering from compromised data and increased liability.

The US Federal Trade Commission gives a list of steps you can take to secure your systems during and after an attack, including consulting a third party data forensics team, securing any physical systems that have been compromised, sorting out any inappropriate material that's been posted on your networks, and talking to the people who found the breach.

Having a sound CSIRP in place is crucial for this phase because following its instructions will ensure that your eradication and security procedures are deep and meticulous, leaving no stone unturned.

Questions to ask at the eradication phase:

1. Have all the malware and affected areas been removed?
2. Have you double-checked all areas that might have been affected?
3. Have you cleaned up any other mess resulting from the attack, such as content posted on your website or media channels?

[9] https://www.ibm.com/security/data-breach

5. Recovery

The recovery phase involves restoring and returning the affected systems back into business operations. This should be done carefully to ensure that another incident doesn't take place.

This process can take days, weeks, or months, depending on the severity of the breach. The NIST recommends starting by immediately strengthening your overall security, and then focusing on long-term, ongoing changes to keep your systems as secure as possible.

Important things to take into consideration during this phase are when to fully restore operations, how you will verify that everything is functioning normally, and how long you will continue to monitor the situation until you're really sure that everything is back to normal.

Questions to ask at the recovery phase:

1. When will systems be back to normal operations?
2. What ongoing tools and procedures will you use to verify that the restored systems are functioning as normal?
3. Can the system be restored from a trusted backup?
4. How long will you monitor the situation until you can be sure that everything is ok?

6. Post-incident activities

This phase essentially consists of a post-incident debrief meeting with all involved parties. The meeting should ideally be held a few days after the incident has been successfully resolved, and no longer than two weeks after, so that everything is fresh in people's minds. It's a way to get closure after the incident.

Key elements of this phase include:

- A complete review of the incident, from discovery to recovery. The review should focus on questions like these: Did everyone follow the procedures in the CSIRP? Was it effective? Were there any weak points or things that could be improved? What could be done differently next time? How could similar incidents be prevented in the future?
- An evaluation and update of your incident plan according to any conclusions drawn from the review.
- The creation of a follow-up report for reference when handling similar incidents. Having a formal chronology of events (with timestamped information like data logs) is also useful for legal procedures like audits.
- An assessment of the total damage caused by the breach, including a monetary estimate. This is also useful for legal reasons such as prosecution activities.
- Tying up all loose ends that you didn't have time for during the incident, such as completing related documentation and making sure that all relevant parties are notified.

Questions to ask at the post-incident activities phase:

1. What changes need to be made to security?
2. What weaknesses did the breach exploit and how can this be prevented in future?
3. Have you thoroughly reviewed the incident and created a follow-up report?
4. Have you notified everybody that needs to be?
5. Have you prepared everything to face the post-incident audit process?

Setting up an incident response team

So, you've created the perfect incident response plan — but who's going to carry it out? That's where you need a dedicated incident response team.

The NIST suggest three different incident response teams models:

- Central — a central body that handles all incidents for the entire organization.
- Distributed — multiple response teams, each responsible for a different physical location, department, or part of the IT infrastructure.
- Coordinated — A central team serving as a knowledge center for various distributed teams, and assisting them with complex, critical or organization-wide incidents.

Depending on the size of your organization and the criticality and complexity of possible incidents, you might have a dedicated, full-time incident response team, or you might train ordinary employees to double as a response team in times of emergency. Some organizations even outsource their security needs to a third-party incident response team.

Questions to ask when setting up a team:

When creating your incident response team, you can ask yourself the following questions to guide the process:

1. Do you need a full-time, dedicated team, or a part-time, "volunteer" team?
2. What training will be necessary for the team? Do they need to be security experts?
3. How much is the training and maintenance of the response team going to cost? It can be expensive, but suffering a major security breach as a result of a poor plan and unprepared team can be considerably more costly, so it's worth the investment.

Get trained to stay ahead of the game

The "ISACA State of Cybersecurity 2021 Part 1" survey found that 61% of organizations feel understaffed in terms of cybersecurity professionals.[10] 50% of respondents felt insufficiently qualified for security positions, and 31% of human resources staff do not understand the criticality of cybersecurity issues. That's probably true of your staff too, right? So getting a good plan in place is essential to raising staff awareness and competence.

Key roles in an incident response team:

Here are some of the key players in a solid incident response team. If you're a smaller company, don't worry! These are roles, not payrolls — that means team members can have multiple roles. In some cases, your team might consist of just one person!

- **Incident response managers** — responsible for approving the CSIRP and coordinating activity when an incident occurs.
- **Security analysts** — review alerts, detect possible incidents, and start investigations when an incident is detected.
- **Threat researchers** — provide contextual information about a threat by searching the web, threat intelligence feeds, data from security tools etc.
- **Other stakeholders** — senior management, board members, HR, PR, and senior security staff such as the Chief Information Security Officer (CISO).
- **Third-parties** — lawyers, outsourced security services, law enforcement agencies etc.

Cybersecurity training exercises

As mentioned in the preparation phase, a core feature of any CSIRP is regular training exercises and drills to keep your team on their toes and ready for any emergency. The purpose of these exercises is to raise staff security awareness, test the effectiveness of your plan and training, and generate discussions among employees.

Your training plan should include at least one large-scale coordinated annual drill, which can be one or two days long. Smaller, table-top drills can be conducted more frequently, according to your organization's needs.

Types of training exercise

Discussion-based exercise

This is a table-top discussion exercise in which your team considers a hypothetical security threat and verbally explores possible response routes.

- **Benefits:** requires minimal preparation and resources, while still putting your team's security knowledge and understanding of their incident response roles to the test in a potential real-life scenario.
- **Drawbacks:** doesn't fully test your response plan or your team's response actions in real-time.

Simulation exercise

This is a live walk-through that has been highly choreographed and planned.

- **Benefits:** tests your team's incident responses in semi-real time, giving them a better understanding of their roles and the criticality of a real-life emergency.
- **Drawbacks:** requires more time to plan and coordinate, but still doesn't completely test your plan or team roles in the most realistic way.

[10] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/new-isaca-study-finds-cybersecurity-workforce-minimally-impacted-by-pandemic-but-still-grappling

Parallel testing

A parallel test is conducted in a safe test environment, making it the most realistic possible type of exercise while still not putting your organization at risk.

- **Benefits:** provides your team with the most realistic simulation and the best real-time feedback about their actions and roles. This should definitely help identify any weak points or holes in your plan and team's role understanding.
- **Drawbacks:** requires more planning than any other type of training, and is also the most expensive because an actual test environment must be simulated (including segregated systems, networks etc.).

Cybersecurity incident response plan best practices

Let's sum up by having a look at these four best practices that should be in place to ensure that your CSIRP is absolutely top notch!

1. Get all stakeholders involved

A security breach can affect all areas of the organization, so you need to make sure that everybody is involved and on board. All key stakeholders should be given a voice in the preparation of your security plan; these can include senior management, human resource leaders, legal representatives, compliance officers, and third-party stakeholders such as technology providers and public relations.

2. Put it to the test

Your security plan might look just marvelous on paper, but it's good for nothing if it doesn't actually work when it needs to. Regular drills and exercises make sure that everybody has a clear idea of what they need to do in an emergency, and they help to identify and remedy any weak spots in the plan. Practice makes perfect!

3. Clarify lines of communication

If you don't have a clear communication strategy in place, a security breach can spell absolute chaos both inside and outside your organization — people start running around like headless chickens, different information is sent to different departments, and nobody has a good idea of what's actually going on. Your communication plan should include clear instructions on who should communicate to whom, using which communication channels, and at what level of detail, for each stage of the incident process. Communications involve not only the incident team but all affected parties including customers and the press, so your strategy should take all of these into consideration as well.

4. Keep it simple

Your incident response plan is like a battle strategy manual, so it should be easy to follow in the heat of war. You don't want your staff to be losing precious time trying to understand an overly-complicated document when your organization is under attack. Yes, it should be detailed, with specific steps and procedures laid out — but it should also be clear and actionable.

How Kaspersky can help

We can help improve your data protection with everything from Kaspersky Optimum Security - which complements your cybersecurity skills in a resource-conscious way, through effective EDR with managed threat hunting, but without prohibitive costs or complexity - to specialist security awareness training, incident response and incident communication services.

Learn More

Further recommended reading

Lessons learned in making remote working work
Ransomware protection in the age of flexible working
A buyer's guide to optimum level of security